Software Engineering Institute

CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1

Kevin G. Partridge
Lisa R. Young

October 2011

TECHNICAL NOTE
CMU/SEI-2011-TN-012

CERT® Program

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by the United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

Contracting Officer
ESC/CAA
20 Shilling Circle
Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

Table of Contents

Abstract

CERT® Resilience Management Model (CERT®-RMM) provides a reference model that allows organizations to make sense of their practice deployment in a process context. In this context, the primary goal of this document is to help model users and adopters to understand how CERT-RMM process areas, industry standards, and codes of practices that are used by organizations in an operational setting are connected. Additionally, this document helps to achieve a primary goal of CERT-RMM, which is to allow adopters to continue to use their preferred standards and codes of practice at a tactical level while maturing management and improvement of operational resilience at a process level. This document was also created with the objective to permit organizations to use CERT-RMM as a means for managing the complexities of deploying more than one standard or code of practice.

1 Introduction

This document is a supplement to the CERT® Resilience Management Model (CERT®-RMM) v1.1. It is primarily intended to help model users and adopters understand the connection between CERT-RMM process areas, industry standards, and codes of practice that are commonly used by organizations in an operational setting.

This document helps to achieve a primary goal of CERT-RMM, which is to allow adopters to continue to use their preferred standards and codes of practice at a tactical level while maturing management and improvement of operational resilience at a process level. This document provides a reference for model adopters to determine how their current deployment of practices supports their desired level of process maturity and improvement.

Another important objective of this document is to permit organizations to use CERT-RMM as a means for managing the complexities of deploying more than one standard or code of practice. CERT-RMM provides a reference model that allows organizations to make sense of their practice deployment in a process context. Thus, issues such as practice overlap and redundancy or the association of a practice to more than one process can be identified and considered to improve processes, reduce practice "quagmires," and improve effectiveness relative to cost. In essence, CERT-RMM can provide organizations a guide for determining the best practices and selectively choosing them based on process improvement goals.

1.1 Model Description

The CERT-RMM v1.1 is a capability maturity model for managing operational resilience. It has two primary objectives:

- Establish the convergence of operational risk and resilience management activities (security planning and management, business continuity, and IT operations and service delivery) into a single model.
- Apply a process improvement approach to operational resilience management by defining and applying a capability scale that expresses increasing levels of process maturity.

1.1.1 Features and Benefits of CERT-RMM

CERT-RMM has the following features:

- provides a process definition, expressed in 26 process areas across four categories—enterprise management, engineering, operations, and process management
- focuses on the resilience of four essential operational assets: people, information, technology, and facilities
- includes processes and practices that define a scale of four capability levels for each process area: incomplete, performed, managed, and defined

® CERT, CERT Resilience Management Model, and CERT-RMM are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

- serves as a meta-model that easily coexists with and references common codes of practice such as ISO2700x, CobiT, BS25999, and ISO24762
- includes quantitative process measurements that can be used to ensure operational resilience processes are performing as intended
- facilitates an objective measurement of capability levels via a structured and repeatable appraisal methodology
- extends the process improvement and maturity pedigree of CMMI to assurance, security, and service continuity activities

A copy of the current version of the CERT Resilience Management Model can be obtained at http://www.cert.org/resilience.

1.2 Relating CERT-RMM to Standards and Codes of Practice

CERT-RMM has several key components. The "process area" forms the major structural element in the model. Each process area has a series of descriptive components.

There are two types of practices referred to in CERT-RMM: specific practices and subpractices. It is important to understand the distinction between these types of practices and the practices contained in common codes of practice in order to make use of this document.

1.2.1 Process Area

CERT-RMM is comprised of 26 process areas. Each process area describes a functional area of competency. In aggregate, these 26 process areas define the operational resilience management system.

1.2.2 Process Area - Process Area Goals

Each process area has a set of goals. Goals are required elements of the process area and define the accomplishment targets of the process that are reflected by the process area. An example of a goal from the Service Continuity process area is "SC:SG1 Prepare for Service Continuity."

1.2.3 Process Area Goals - Specific Practices

The process area goals are decomposed into specific practices. Specific practices are expected elements of the process area that, when achieved, should promote accomplishment of the associated goal. Specific practices are considered to be the "base practices" of the process area that reflect the area's body of knowledge. An example of a specific practice from the Service Continuity process area is "SC:SG1.SP1 Plan for Service Continuity," which is a practice aimed at the achievement of goal "SC:SG1 Prepare for Service Continuity."

1.2.4 Specific Practices - Subpractices

Specific practices are decomposed into subpractices. Subpractices are informative elements associated with each specific practice and relevant process work products. Subpractices are a transition point for process area specific practices because the focus changes at this point from "what" must be done to "how." While not overly prescriptive or detailed, subpractices help the user to determine how to satisfy the specific practices and achieve the goals of the process area. Each

organization will have its own subpractices either organically developed by the organization or acquired from a code of practice.

1.2.5 Subpractices - Standards and Common Codes of Practice

Subpractices can be linked to standards and codes of practice.[1] Subpractices are typically generic in nature, while codes of practice can be very specific. For example, a subpractice may suggest "set password standards and guidelines" while a specific code of practice may state that "passwords should be changed at 90-day intervals."

[1] Standards and codes of practice are not universally written at the implementation level. Thus, some standards and codes of practice may include elements of goals, specific practices, and subpractices. However, generally standards and codes of practice provide implementation details that can be used to actualize CERT-RMM goals and specific practices, and therefore are considered to be comparable to subpractices in the CERT-RMM model.

2 Standards and Codes of Practice

This section details the standards and codes of practice that have been referenced in this document. These standards and codes are typically in the public domain but may have usage and license restrictions. For ease of use, practices have been referenced by their original numbers, but there is no restatement of the practice included. Information on obtaining copies of each code of practice is included in this section, as each copyright owner (or licensor) is the authoritative source for the respective standard or code of practice.[2]

2.1 ANSI/ASIS SPC.1-2009

The ANSI/ASIS SPC.1-2009 is the American National Standard on Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use [ANSI 2009]. The document is published by ASIS International and approved by the American National Standards Institute, Inc. The standard is designed as an organizational resource to foster preparedness in anticipation of disruptive incidents. The standard presents guidelines on its interpretation of organizational resilience management.

The ANSI/ASIS SPC.1-2009 can be obtained in PDF from ASIS online at http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf.

2.2 BS 25999

BS 25999 is the British Standards Institution's (BSI) code of practice and specification for business continuity management. The purpose of the standard is to provide a basis for understanding, developing, and implementing business continuity within an organization and to provide confidence in the organization's dealings with customers and other organizations.

There are two BS 25999 documents: the code of practice, BS 25999-1:2006 [BSI 2006], and the specification, BS 25999-2: 2007 [BSI 2007]. The code of practice was used for the crosswalk in this document.

British Standards can be obtained in PDF or hard copy format from the BSI online shop at http://www.bsigroup.com/Shop. Hard copies can also be obtained by contacting BSI Customer Services at +44 (0)20 8996 9001 or cservices@bsigroup.com.

2.3 COBIT 4.1

COBIT is the Control Objectives for Information and Related Technology [ITGI 2007]. It was developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) to provide managers, auditors, and IT users with generally accepted in-

[2] The copyright owners of the codes of practice have not participated in the creation or review of CERT RMM or this Code of Practice Crosswalk. Accordingly, the inclusion of a particular standard or code of practice in this Code of Practice Crosswalk is not an endorsement or validation of the Software Engineering Institute, CERT RMM or this Code of Practice Crosswalk by such copyright owner, and all references to such codes of practice should be read as qualified by the actual codes of practice.

formation technology control objectives to maximize IT benefits and ensure appropriate IT governance, security, and control.

COBIT 4.1 is the current version and was used in this crosswalk document. Further information regarding the implementation of COBIT 4.1, including copies of the current version, can be obtained by visiting http://www.isaca.org and http://www.itgi.org.

2.4 CMMI

Capability Maturity Model® Integration (CMMI®)[3] is a process improvement maturity model for the development of products and services. The CMMI for Development (CMMI-DEV) represents the systems and software development domain [CMMI 2006]. The CMMI for Services (CMMI-SVC) constellation is designed to cover the activities required to manage, establish, and deliver services [CMMI 2009].

CMMI for Development v1.2 is used in this document and is referenced as CMMI-DEV. It can be obtained at http://www.sei.cmu.edu/library/abstracts/reports/06tr008.cfm. CMMI for Services v1.2 is used in this document and can be obtained at http://www.sei.cmu.edu/library/abstracts/reports/09tr001.cfm. It is referenced as CMMI-SVC throughout this document.

2.5 FFIEC Business Continuity Planning Handbook

The Federal Financial Institutions Examination Council (FFIEC) publishes a series of booklets that comprise the FFIEC Information Technology Examination Handbook. These booklets are published to help bank examiners to evaluate financial institutions and service provider risk management processes with the goal of ensuring the availability of critical financial services.

The FFIEC Business Continuity Planning booklet [FFIEC 2008] was used for reference in this code of practice crosswalk. In the future, the FFIEC Information Security booklet will be referenced as well. FFIEC booklets can be obtained at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

2.6 ISO/IEC 20000-2:2005 (E)

ISO/IEC 20000 is a standard and code of practice for IT service management published by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). It is based on (and supersedes) the earlier British Standard BS 15000. It reflects the best practice guidance for IT service management as provided in the ITIL (Information Technology Infrastructure Library) framework, but also broadly covers other service management standards.

The ISO/IEC 20000-2:2005 code of practice [ISO/IEC 2005a] was used in this crosswalk document. The standard ISO/IEC 20000-1:2005 and the code of practice ISO/IEC 20000-2:2005 can be purchased from ANSI at http://webstore.ansi.org/.

[3] Capability Maturity Model and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

2.7 ISO/IEC 24762:2008 (E)

ISO/IEC 24762, “Guidelines for information and communications technology disaster recovery services” [ISO/IEC 2008a], is part of business continuity management standards published by ISO/IEC. It can be applied in-house or to outsourced providers of DR physical facilities and services.

The current version of the standard, ISO/IEC 24762:2008, can be purchased from ANSI at http://webstore.ansi.org/.

2.8 ISO/IEC 27002:2005 (E)

ISO/IEC 27002, “Code of practice for information security management” [ISO/IEC 2005b], broaches the full scope of security management, at points touching upon both IT management and disaster recovery. ISO/IEC 27002 is part of a growing “27000 series” that evolved from the original British Standard BS 7799, which was translated to ISO standard ISO 17799.

The current version of the code of practice, ISO/IEC 27002:2005, can be purchased from ANSI at http://webstore.ansi.org/.

2.9 ISO/IEC 27005:2008 (E)

ISO/IEC 27005, “Information technology – Security techniques – Information security risk management” [ISO/IEC 2008b], is also a British Standard derivation. ISO/IEC 27005 is based upon BS 7799-3:2006. The standard describes a risk management process specific to information security and analysis of that risk.

The current version of the code of practice, ISO/IEC 27005:2008, can be purchased from ANSI at http://webstore.ansi.org/.

2.10 ISO/IEC 31000:2009 (E)

ISO/IEC 31000, “Risk Management – Principles and Guidelines” [ISO/IEC 2009], is another standard published by ISO/IEC and, as mentioned, is distinct from ISO/IEC 27005. ISO/IEC 31000 deviates from the British Standard origin of the preceding standards. ISO/IEC is derived from the Standards Australia and Standards New Zealand document: AS/NZS 4360:2004. This standard is a set of best practices and guidelines for the development of a risk management framework. The framework guidance is organizational in scope and focuses on the management of perceptible risk and risk tolerance.

The current version of the code of practice, ISO/IEC 31000:2009, can be purchased from ANSI at http://webstore.ansi.org/.

2.11 NFPA 1600

NFPA 1600 is the National Fire Protection Agency Standard on Disaster/Emergency Management and Business Continuity Programs [NFPA 2007]. It is primarily focused on the development, implementation, and operation of disaster, emergency, and business continuity programs, including the development of various types of related plans. The 2007 edition of this standard was used for reference and is an update of the 2004 standard.

The standard can be obtained at the NFPA website at http://www.nfpa.org.

2.12 PCI DSS

PCI DSS is the Payment Card Industry Data Security Standard that evolved from security efforts by major credit card organizations [PCI 2009]. It is intended to provide a data security standard for merchants and card payment service providers and processors to prevent fraud and control vulnerabilities. Compliance with the standard is validated through assessments performed by PCI DSS-qualified assessors.

The current standard version is 1.2.1.[4] It can be downloaded at http://www.pcisecuritystandards.org.

[4] Payment Card Industry (PCI) Data Security Standard, Version 1.1 (Release: September 2006) provided courtesy of PCI Security Standards Council, LLC and/or its licensors. © 2007 PCI Security Standards Council, LLC. All Rights Reserved.

3 RMM Crosswalk

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ADM – Asset Definition and Management													
ADM:SG1 Establish Organizational Assets													
ADM:SG1.SP1 Inventory Assets Subpractices 1. Identify and inventory vital staff. 2. Identify and inventory high-value information assets. 3. Identify and inventory high-value technology components. 4. Identify and inventory high-value facilities. 5. Develop and maintain an asset database that establishes a common source for all high-value assets.		7.7.1	CM:SP1.1	CM:SP1.1	PO4.13		6.6.2 9.1.1 9.1.2	5.3.1 5.3.2 5.3.3 5.5.3 6.14.9 7.14.6	7.1.1 15.1.3	8.2.1.2		6.1.3 6.1.5 6.1.6	12.3.4 12.3.7

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ADM:SG1.SP2 Establish A Common Understanding Subpractices 1. Create an asset profile for each asset (or similar work product) and document a common description. 2. Describe and document the "acceptable use" of the asset. Ensure alignment between acceptable uses and resilience requirements. 3. Classify information assets as to their level of sensitivity. 4. Update the asset database with asset profile information.					PO2.1 PO2.2		4.1.1 6.6.2	5.5.3	7.1.1 7.1.3 7.2.1 10.1.1				1.1.9 3.2 12.3

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ADM:SG1.SP3 Establish Ownership and Custodianship Subpractices 1. Document and describe the owner of each asset on the asset profile (or similar work product). 2. Group assets that are collectively needed to perform a specific business process or service, and identify service owners, if necessary. 3. Document and describe the physical location of the asset and the custodian of the asset.		7.7.2			PO4.9		4.1.1 4.1.4 6.6.2	5.3.2 5.3.3	6.1.3 7.1.1 7.1.2 11.6.2	8.2.1.2			1.1.8 12.3.8

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ADM:SG2 Establish the Relationship Between Assets and Services													
ADM:SG2.SP1 Associate Assets with Services Subpractices 1. Identify high-value services. 2. Assign assets in the asset database to one or more services. 3. Update asset profiles to establish and document the asset's association to a service. 4. Update the asset database with asset-to-service association information.		6.1.1 7.7.1	CM:SP3.1	CM:SP3.1			4.1.1 4.1.2 4.1.4 6.6.2	5.3.1 5.3.2	7.1.1 7.1.2 11.6.2				7.2 6.3.2 6.3.3 12.3.8 16.5

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ADM:SG2.SP2 Analyze Asset-Service Dependencies Subpractices 1. Identify asset dependencies and potential conflicts. 2. Develop mitigation plans to reduce the effects of dependencies that could affect the operational resilience of associated services. 3. Implement actions to reduce or eliminate conflict.		6.1.1 7.7.1					4.1.2	6.14.8	7.1.2 11.6.2				6.1.1 6.1.2
ADM:SG3 Manage Assets													
ADM:SG3.SP1 Identify Change Criteria Subpractices 1. Establish an asset inventory baseline from which changes will be managed. 2. Develop and document criteria for establishing when a change in asset inventory must be considered.			CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1	CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1	PO10.11		4.1.2 4.1.3					6.1.5	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ADM:SG3.SP2 Maintain Changes to Assets and Inventory Subpractices 1. Document the asset changes by updating asset profiles and the asset database. 2. Maintain a requirement change history with rationale for performing the changes. 3. Evaluate the impact of asset changes on existing resilience requirements and activities and commitments for protecting and sustaining assets. 4. Establish communication channels to ensure custodians are aware of changes in assets.			CM:SP3.2	CM:SP3.2	PO10.11		4.1.2 4.1.4 5.2	7.14	9.2.6			6.1.5 6.1.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
AM – Access Management													
AM:SG1 Manage and Control Access													
AM:SG1.SP1 Enable Access Subpractices 1. Establish access management policies and procedures. 2. Complete and submit access requests. 3. Approve access requests. 4. Provide users [access holders] with a written statement of their access rights and responsibilities. 5. Implement access requests.					DS5.3 DS5.4 DS12.3	Other Policies, Standards, and Pro-cesses		5.7.3 6.3.1-7 6.3.12-14 6.4.8 6.4.9 6.12.1 6.12.2.2 6.12.5.5 7.5.1 7.5.7	6.1.4 6.2.2 9.1.1,2 10.1.4 10.8.5 10.9.1,3 11.1.1 11.2 11.3.1 11.4.1,2,3 11.4.6,7 11.5.1,3,4 11.6.1 11.7.1,2 12.3.2 12.4.3 15.1.5 15.3.2			4.8.2 6.4.4	7.1 7.2 8.1 12.5.8

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
AM:SG1.SP2 Manage Changes to Access Privileges Subpractices 1. Establish an enterprise-wide change management process for access privileges. 2. Establish organizational criteria that may signify changes in access privileges. 3. Manage changes to access privileges.					DS5.4 PO7.8 DS12.3	Other Policies, Standards, and Pro-cesses		6.4.8 6.4.9 7.5.3 7.5.4 7.5.5	6.2.2 9.1.2 10.8.5 11.2,3 11.5.4 12.3.2 15.3.2				7.1.2 7.1.3 7.2.6 12.5.8
AM:SG1.SP3 Periodically Review and Maintain Access Privileges Subpractices 1. Establish regular review cycle and process. 2. Perform periodic review of access privileges by asset. 3. Identify inconsistencies or misalignments in access privileges.					DS5.4 DS12.3			6.3.10 6.4.8 6.4.9 7.5.3 7.5.4	6.2.2 9.1.2 11.2.4 12.3.2 15.3.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
AM:SG1.SP4 Correct Inconsistencies Subpractices 1. Develop corrective actions to address excessive or inappropriate levels of access privileges. 2. Correct access privileges as required. 3. Document disposition for excessive or inappropriate levels of access privileges that will not result in changes or deprovisioning. 4. Identify risks related to excessive or inappropriate levels of access privileges. 5. Update status on corrective actions.					PO7.8 DS12.3				9.1.2 11.2.4 15.3.2				6.1

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM – Communications													
COMM:SG1 Prepare for Resilience Communications													
COMM:SG1.SP1 Identify Relevant Stakeholders Subpractices 1. Identify relevant stakeholders that may have a vested interest or vital role in communications about resilience. 2. Establish a plan that describes the involvement of all communications stakeholders.		8.5.6	IPM:SP2	IPM:SP2	PO6.5	Appendix G: BCP Compo-nents						5.1.4 5.2.9 6.3.8	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG1.SP2 Identify Communications Requirements Subpractices 1. Analyze the resilience program to identify the types and extent of communication that is necessary to satisfy resilience program objectives. 2. Document the communications needs of stakeholders. 3. Establish communications requirements for the operational resilience management processes. 4. Analyze and prioritize communication requirements. 5. Revise the communication needs of the organization as changes to the resilience program and strategy are made.			IPM:SP2	IPM:SP2		Other Policies, Standards, and Pro-cesses Appendix G: BCP Compo-nents		5.8.3				5.2.9 6.3.1 6.3.7 6.11.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG1.SP3 Establish Communications Guidelines and Standards Subpractices 1. Develop resilience communication guidelines and standards.		8.5.5 DS5.11	IPM:SP2	IPM:SP2		Other Policies, Standards, and Pro-cesses		5.8.3				5.2.9 6.3.3	
COMM:SG2 Prepare for Communications Management													
COMM:SG2.SP1 Establish a Resilience Communications Plan Subpractices 1. Develop and implement a resilience communications plan. 2. Establish commitments to the communications plan. 3. Revise the plan and commitments as necessary.	4.3.2 4.4.2	8.5.5				Appendix G: BCP Compo-nents		5.8.3 6.7.3 6.7.6		11		5.2.9 6.3.2 6.3.7 6.4.6	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG2.SP2 Establish a Resilience Communications Program Subpractices 1. Establish a resilience communications program.	4.4.2				PO6.5	Appendix G: BCP Compo-nents		6.7.3				6.3.3 6.3.4 6.3.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG2.SP3 Identify and Assign Plan Staff Subpractices 1. Develop detailed job descriptions for each role/responsibility detailed in the communications plan. 2. Establish a list of candidate and skilled resources to fill each role/responsibility in the communications plan. 3. Assign resources to communication processes roles and responsibilities. 4. Ensure that organizational training is provided to communications staff with respect to the specific resilience communication roles they perform.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG3 Deliver Resilience Communications													
COMM:SG3.SP1 Identify Communications Methods and Channels Subpractices 1. Inventory communications methods and channels that currently exist. 2. Identify the appropriate communications methods and channels for each type of stakeholder. 3. Identify communication methods and channels that do not currently exist. 4. Identify tools, techniques, and methods required to use the identified methods and channels.					PO6.5 DS5.11		6.2.1 6.6.6	6.7.6 6.11.3.2				6.3.3 6.3.7 6.3.8	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:3.SP2 Establish and Maintain Communications Infrastructure Subpractices 1. Identify and inventory existing communications infrastructure and capabilities that may be able to meet plan and program objectives and communications requirements. 2. Identify infrastructure needs to support communications requirements, methods, and channels. 3. Implement and maintain communications infrastructure.					PO6.5		6.2.1	6.7.1 6.7.2 6.7.5 6.7.6 6.11.3.2				6.3.3 6.3.5 6.3.6 6.3.7 6.3.8	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG4 Improve Communications													
COMM:SG4.SP1 Assess Communications Effectiveness Subpractices 1. Establish and implement a formal communications review activity. 2. Prepare an analysis report on the effectiveness of the communications activities. 3. Compare outcomes of communications processes with plan objectives and expectations. 4. Document suggested improvements to the communications plan and program based on the evaluation of the effectiveness of awareness activities.												6.3.3 7.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMM:SG4.SP2 Improve Communications Subpractices 1. Review results of communications assessment activities and effectiveness analysis reports. 2. Review communication processes, plans, and programs and update for any perceived deficiencies or omissions. 3. Revise the communication methods, channels, and supporting work products as necessary.			IPM:SP2	IPM:SP2									

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP – Compliance													
COMP:SG1 Prepare for Compliance Management													
COMP:SG1.SP1 Establish a Compliance Plan Subpractices 1. Develop a strategic plan for managing compliance. 2. Establish sponsorship and resource commitments for the compliance plan. 3. Revise the plan and commitments on a cycle commensurate with the organization's strategic planning process.			VER:SP1.2 VER:SP2.1		ME3.1			6.14.6.1 6.15.1				4.5.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG1.SP2 Establish a Compliance Program Subpractices 1. Establish a compliance program. 2. Assign resources to compliance program. 3. Provide funding for the compliance program. 4. Provide sponsorship and oversight to the compliance program.			VER:SP1.2 VER:SP2.1					6.14.6.1 6.15.1 6.15.4				4.5.2	
COMP:SG1.SP3 Establish Compliance Guidelines and Standards Subpractices 1. Develop and communicate compliance guidelines and standards.			VER:SP1.3		ME3.2 PO6.4	Appendix A: Exami-nation Procedures		6.14.6.1 6.14.6.3 6.15.2	5.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG2 Establish Compliance Obligations													
COMP:SG2.SP1 Identify Compliance Obligations Subpractices 1. Interview service owners, auditors, and legal to identify compliance obligations. 2. Identify compliance obligations that the organization may have to satisfy because of its external entity affiliations. 3. Identify internal policies and procedures that should be included in the inventory of compliance obligations. 4. Identify sources of potential new compliance obligations. 5. Develop an inventory of compliance obligations.					PO3.3 ME3.1 ME4.7	Business Impact Analysis Other Policies, Standards, and Processes Appendix A: Examination Procedures Appendix I: Laws, Regulations, and Guidance	4.1.3 6.2.1 6.6.6 9.1.5	6.10.2 6.14.3 6.15.2 6.15.3 7.6.3	15.1.1 15.2.1 6.1.2			5.2.2 5.4.3 6.11.6	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG2.SP2 Analyze Obligations Subpractices 1. Establish technique for performing analysis on compliance obligations. 2. Analyze compliance obligations and document results. 3. Identify conflicting obligations.			PPQA:SP1.1 VER:SP2.2 VER:SP3.1	PPQA:SP1.1	PO3.3 ME3.2		4.1.3					5.4.3	
COMP:SG2.SP3 Establish Ownership for Meeting Obligations Subpractices 1. Establish the owner for each compliance obligation. 2. Establish training requirements for compliance roles, if necessary. 3. Identify compliance obligations that have not been assigned or accepted.			PPQA:SP2.1	PPQA:SP2.1	PO4.8 DS5.2			6.10.3 6.14.6.1	15.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG3 Demonstrate Satisfaction of Compliance Obligations													
COMP:SG3.SP1 Collect and Validate Compliance Data Subpractices 1. Develop strategies for data collection and validation. 2. Establish compliance knowledgebase or information repository. 3. Implement processes for data validation and integrity checking.			VER:SP2.3 VER:SP3.2		ME4.7 DS5.5 ME2.4	Appendix A: Examination Procedures	9.1.5	6.14.6.1	15.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG3.SP2 Demonstrate the Extent of Compliance Obligation Satisfaction Subpractices 1. Establish minimum requirements for compliance. 2. Determine the stakeholders of the compliance reports and data. 3. Prepare and submit compliance reports as necessary. 4. Track progress against compliance obligations and identify obligations that may not be met on time. 5. Identify risks and potential costs of non-compliance. 6. Identify areas that may need remediation for compliance purposes. 7. Gather performance data on the achievement of compliance obligations.					ME3.5 ME4.7 DS5.5	Appendix A: Exami-nation Procedures	9.1.5		15.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG3.SP3 Remediate Areas of Non-Compliance Subpractices 1. Identify areas of suggested remediation. 2. Analyze areas of suggested remediation and develop detailed remediation plans. 3. Assign resources to perform remediation. 4. Track remediation activities to completion. 5. Assess remediation activities to determine if satisfaction of compliance obligations has been achieved. 6. Update satisfaction of compliance obligations (as a result of remediation), if appropriate.			PPQA:SP2.1	PPQA:SP2.1	ME3.4 ME4.7 DS5.5			6.10.2	15.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
COMP:SG4 Monitor Compliance Activities													
COMP:SG4.SP1 Evaluate Compliance Activities Subpractices 1. Establish and maintain clearly stated criteria for evaluations. 2. Evaluate compliance processes for adherence to compliance standards and guidelines for meeting compliance obligations using the stated criteria. 3. Identify deficiencies and areas for improvement, particularly where the satisfaction of compliance obligations has been impaired. 4. Identify and apply lessons learned that could improve the organization's compliance process.	4.5.2.1				ME3.2 ME3.3			6.14.6.2	15.2.2			4.5.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
CTRL – Controls Management													
CTRL:SG1 Establish Control Objectives													
CTRL:SG1.SP1 Define Control Objectives Subpractices 1. Identify management directives and organizational guidelines upon which to base the definition of control objectives. 2. Define and document control objectives that result from management directives and guidelines. 3. Prioritize control objectives.					AI2.3 PO6.1 PO6.2 PO10.12			6.4.1 6.4.2 6.4.3.1 6.4.3.2	10.4 10.5 10.6 10.7 12.3.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
CTRL:SG2 Establish Controls													
CTRL:SG2.SP1 Define Controls Subpractices 1. Establish enterprise-level controls to satisfy control objectives. 2. Confirm or assign responsibility for implementing enterprise-level controls. 3. Establish service- and asset-level controls to satisfy control objectives. 4. Confirm or assign responsibility for implementing service- and asset-level controls. 5. Develop a bi-directional traceability matrix that maps control objectives and enterprise-, service-, and asset-level controls.								6.4.1 6.4.2 6.4.3.1 6.4.3.2	10.4,5,6,7 11.2,3,4,5 11.6,7 12.3.1				9.2 9.3

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
CTRL-3: Analyze Controls													
CTRL:SG3.SP1 Analyze Controls Subpractices 1. Analyze existing controls against control objectives. 2. Identify gaps where an existing control does not fully meet one or more control objectives. 3. Identify gaps where enterprise control objectives for the resilience of services, assets, and service control objectives are not adequately satisfied by existing controls. 4. Identify updates to existing controls and proposed new controls to address gaps. 5. Identify redundant and conflicting controls and changes to address them. 6. Identify risks that may result from unsatisfied control objectives as well as redundant and conflicting controls.					AI3.2 AI2.3 ME2.3 ME2.4					8.2.1.4			

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
CTRL:SG4 Assess Control Effectiveness													
CTRL:SG4.SP1 Assess Controls Subpractices 1. Select the scope for the assessment. 2. Perform the assessment. 3. Identify problem areas. 4. Identify updates to existing controls and proposed new controls to address problem areas. 5. Identify updates to service continuity plans that may result from changes to the internal control system. 6. Identify risks that may result from unresolved problems.					AI3.2 AI2.3 ME2.5				6.1.2 6.1.8	8.2.1.4			

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC – Environmental Control													
EC:SG1 Establish and Prioritize Facility Assets													
EC:SG1.SP1 Prioritize Facility Assets Subpractices 1. Compile a list of high-value facility assets from the organization's asset inventory. 2. Prioritize facility assets. 3. Periodically validate and update the list of critical facility assets based on operational and organizational environment changes.		6.4				Appendix G: BCP Compo-nents							

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG1.SP2 Establish Resilience-Focused Facility Assets Subpractices 1. Compile a list of resilience-focused facility assets from the organization's asset inventory. 2. Periodically reconcile the list of resilience-focused facilities to the organization's services continuity plans and resilience-focused strategies.		6.4 8.5.7			DS4.8	Appendix G: BCP Compo-nents	9.1.2	6.1 6.4.7 6.5 6.6.1,3 6.8.4 6.10.1 6.11.3.3 6.11.3.4 6.11.4 6.12.1 6.12.2.3 6.12.5.2 6.12.7, 8 6.13.2,3,4 6.14.1	9.1			6.1.4 6.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG2 Protect Facility Assets													
EC:SG2.SP1 Assign Resilience Requirements to Facility Assets Subpractices 1. Assign resilience requirements to facility assets. 2. Document the requirements (if they are currently not documented) and include in the asset definition.					DS12.1 DS12.2 DS4.8			5.4 5.3.3 5.7.1 6.2 6.3.1 6.4.1,2 6.4.3.1, 3.2 6.4.5.4 6.4.7 6.4.10,11 6.4.12,13 6.5 6.6.1,3 6.10.1,4 6.12.2.3 6.12.5.2	6.2.2 6.2.3 6.2.4 6.2.5 6.2.6 6.2.7 6.2.8 6.2.9				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG2.SP1 Assign Resilience Requirements to Facility Assets Subpractices 1. Assign resilience requirements to facility assets. 2. Document the requirements (if they are currently not documented) and include in the asset definition.								6.12.7,8 6.13.2,3,4 6.14.2 6.6.3					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG2.SP2 Establish and Implement Controls Subpractices 1. Establish and implement administrative controls for facility assts. 2. Establish and implement technical controls for facility assets. 3. Establish and implement physical controls for facility assets. 4. Establish and specify controls over the design, construction, or leasing (acquisition) of facility assets. 5. Monitor the effectiveness of administrative, technical, and physical controls, and identify deficiencies that must be resolved.					DS12.1 DS12.2 DS12.3 DS12.4			5.4 5.7.1 6.3 6.4.1 6.4.2 6.4.3.1 6.4.3.2 6.4.3.3 6.4.5,7 6.4.10,11 6.4.12,13 6.6.1 6.8.5.4,5 6.9.2 6.10.1,4 6.12.2.3 6.12.2,5,6 6.12.7,8 6.13.2,3,4 6.14.2	9.1 9.2.1,3,4,5 9.2.7 10.1.1,3,4 10.6.1 10.8.5 11.6.2 11.7.1,2 15.1.3,4 15.3.2				13.1

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG3 Manage Facility Asset Risk													
EC:SG3.SP1 Identify and Assess Facility Asset Risk Subpractices 1. Determine the scope of risk assessment for facility assets. 2. Identify risks to facility assets. 3. Analyze risks to facility assets. 4. Categorize and prioritize risks to facility assets. 5. Assign a risk disposition to each facility asset risk. 6. Monitor the risk and the risk strategy on a regular basis to ensure that it does not pose additional threat to the organization. 7. Develop a strategy for those risks that the organization decides to mitigate.					DS12.2	Risk Man-agement		6.7.1 6.7.3,4,5 6.8.1,3,4 6.8.5.1,2,3 6.9.3 6.14,15 8.2 9.4.2	6.2.2 6.2.3,4,5 6.2.6,7,8,9 11.7.1,2			5.4.3 5.6.1 5.6.2 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG3.SP2 Mitigate Facility Risks Subpractices 1. Develop and implement risk mitigation strategies for all risks that have a "mitigation" or "control" disposition. 2. Validate the risk mitigation plans by comparing them to existing protection and sustainability strategies. 3. Identify the person or group responsible for each risk mitigation plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan. 4. Address residual risk. 5. Implement the risk mitigation plans and provide a method to monitor the effectiveness of these plans. 6. Monitor risk status. 7. Collect performance measures on the risk management process.					DS12.2	Risk Man-agement		6.2.10	9.1 11.7.1 11.7.2			5.6.1 5.6.2 5.6.3 5.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG4 Control Operational Environment													
EC:SG4.SP1 Perform Facility Sustainability Planning Subpractices 1. Perform business impact analysis. 2. Develop service continuity plans that address facility availability.		7.4			DS12.1		6.3.4	6.1 6.6.1	9.1.1 9.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG4.SP2 Maintain Environmental Conditions Subpractices 1. Identify control systems that require regular maintenance. 2. Document equipment supplier's recommended service intervals and specifications. 3. Document a list of maintenance personnel authorized to carry out repairs and service. 4. Document all suspected or actual faults and all preventative, corrective, and other types of maintenance. 5. Implement maintenance and test maintenance changes in a non-operational environment. 6. Establish appropriate controls over sensitive or confidential information when maintenance is performed. 7. Communicate maintenance change notification to appropriate entities.					DS12.4 DS12.5			5.2 5.3.3 6.1,2 6.3.8 6.6.1,2 6.6.4 6.9.3 6.10.4,5 6.12.2,3,4 6.14 6.14.6.4 6.14.8 6.14.11	9.1.1 9.2.1,2,4					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG4.SP2 Maintain Environmental Conditions Subpractices (continued) 8. Implement maintenance according to change request procedures. 9. Document and communicate results of maintenance.													
EC:SG4.SP3 Manage Dependencies on Public Services Subpractices 1. Identify and document public services on which facilities rely. 2. Develop a key contact list for organizational services that can be included as part of service continuity plans.		8.5.8		SD:SP1.1 SD:SP1.2 SD:SP2.1 SD:SP2.2 SD:SP2.3 SD:SP3.3		Risk Man-agement	6.1.2 6.3.4	5.5.1 5.8.2,4,5 6.1 6.2.8 6.2.9 6.8.2 6.10.5	6.1.6 9.2.1,2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG4.SP4 Manage Dependencies on Public Infrastructure Subpractices 1. Identify and document internal infrastructure dependencies that the organization relies upon to provide services. 2. Identify and document external resources that the organization relies upon to provide services. 3. Develop a key contact list for public infrastructure services that can be included as part of the service continuity plans. 4. Update service continuity plans as appropriate.				SD:SP1.1 SD:SP1.2 SD:SP2.1 SD:SP2.2 SD:SP2.3 SD:SP3.3		Risk Management	6.1.2 6.3.4	5.5.1 5.8.2,3,4,5 6.1 6.2.8,9 6.7.5 6.8.2 6.9.3 6.10.5	6.1.6 9.2.1 9.2.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EC:SG4.SP5 Plan for Facility Retirement Subpractices 1. Develop a plan for facility retirement. 2. Develop and implement service continuity plans to support the retirement of the facility asset. 3. Archive facility work products. 4. Retire the facility by executing the retirement plan.								6.14.7	9.2.6				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF – Enterprise Focus													
EF:SG1 Establish Strategic Objectives													
EF:SG1.SP1 Establish Strategic Objectives Subpractices 1. Identify the organization's mission, vision, values, and purpose. 2. Identify the organization's strategic objectives.		6.1.1	DAR:SP1.1 IPM_IPPD: SP3.1	DAR:SP1.1	PO1.2 PO1.4 ME4.2	Board and Senior Manage-ment Re-sponsibility			5.1.1			5.1.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG1.SP2 Establish Critical Success Factors Subpractices 1. Collect data to support the development of critical success factors. 2. Consolidate and analyze critical success factor data. 3. Derive the critical success factors for the organizations. 4. Perform affinity analysis between strategic objectives and critical success factors. 5. Identify the key performance indicators to measure accomplishment of each critical success factor. 6. Monitor the accomplishment of critical success factor and take corrective action as necessary.		6.1.1 6.1.2	DAR:SP1.2	DAR:SP1.1	PO1.2 ME4.2	Business Impact Analysis						5.5.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG1.SP3 Establish Organizational Services Subpractices 1. Inventory organizational services and develop service repository. 2. Document service attributes in a service profile. 3. Perform affinity analysis between organizational services and objective measures such as strategic objectives and critical success factors. 4. Define high-value services from the organization's standard services repository. 5. Revise the organization's service profiles and services repository and service levels as necessary.		6.1.1 6.1.2 6.3			PO1.2	Board and Senior Manage-ment Re-sponsibility Business Impact Analysis	3.1 4.1.4 5.1 5.2 6.1.1,2 6.1.3,4 7.3.3						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG2 Plan for Operational Resilience													
EF:SG2.SP1 Establish an Operational Resilience Management Plan Subpractices 1. Develop the resilience management plan. 2. Establish commitments to the plan. 3. Revise the plan and commitments on a cycle commensurate with the organization's strategic business planning process.	4.4.4		PP:SP2.7		PO1.5 PO6.3 DS5.2	Board and Senior Manage-ment Re-sponsibility	3.1 4.1.4 6.6.6		5.1.1 6.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG2.SP2 Establish an Operational Resilience Management Program Subpractices 1. Establish the operational resilience management program. 2. Fund the operational resilience management program. 3. Assign resources to the operational resilience management program. 4. Provide oversight to the operational resilience management program. 5. Gather performance data on the achievement of strategic resilience objectives.	4.1.1 4.4.4				PO1.5 PO1.6 PO4.4 PO4.5 PO4.6 PO4.7	Board and Senior Manage-ment Re-sponsibility	3.1 4.1.4 6.6.6		5.1.1 6.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG3 Establish Sponsorship													
EF:SG3.SP1 Commit Funding for Operational Resilience Management Subpractices 1. Develop the business case for the operational resilience management program and process. 2. Establish operational resilience management program and process funding as a regular part of the organization's strategic plan budgeting (capital and expense) exercise. 3. Approve allocation of funding to operational resilience management program and process activities.	4.4.1				PO1.1 DS5.2		3.1 4.1.4		6.1.1 14.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG3.SP2 Promote a Resilience-Aware Culture	4.4.2	5.4.2 10.1					6.6.6		6.1.1 10.9			4.1.1 4.1.2	
Subpractices 1. Establish a plan for visible promotion of a resilience-aware culture with appropriate success metrics. 2. Establish performance management of higher level managers for resilience. 3. Establish rewards and recognition programs to support resilience acculturation. 4. Measure to the extent possible the level of acculturation of resilience awareness that is the direct result of sponsorship.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG3.SP3 Sponsor Resilience Standards and Policies Subpractices 1. Establish policy statements reflecting senior management's commitment to managing resilience.	4.2.1	5.2 10.1			PO6.1 DS5.1		3.1 3.2 6.6.6		5.1.1 6.1.1 7.1.3 11.6.1			4.1.1 4.1.2 4.1.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG4 Provide Resilience Oversight													
EF:SG4.SP1 Establish Resilience as a Governance Focus Area Subpractices 1. Establish a governance framework for the operational resilience management system. 2. Assign roles and responsibilities for governance over the operational resilience management system. 3. Identify the procedures, policies, standards, guidelines, and regulations that will form the basis for resilience governance activities.	4.4.1	5.2.1			PO1.6 PO4.2 PO4.3 ME4.1 DS5.1				5.1.2			4.3.1 4.3.2 4.3.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG4.SP2 Perform Resilience Oversight Subpractices 1. Identify key governance stakeholders. 2. Establish governance dashboard or scorecard for measuring and managing operational resilience management system performance. 3. Monitor and collect data for measuring key indicators and metrics and reporting on these indicators to key stakeholders. 4. Review audit reports on a regular basis for indicators of problems. 5. Establish a process for handling exceptions to the organization's acceptable behaviors. 6. Establish reporting procedures to communicate results of measurement against indicators to governance stakeholders. 7. Provide reports on performance to governance stakeholders.		5.2.2			PO1.6 PO4.2 PO4.3 ME4.6 DS5.1		3.1 3.2		5.1.2			4.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EF:SG4.SP3 Establish Corrective Actions Subpractices 1. Identify and analyze (measurements of) key indicators that do not meet established metrics. 2. Develop corrective actions to close perceived gaps. 3. Identify persons or groups responsible for implementing and managing corrective actions. 4. Report on the success of the corrective actions to key stakeholders. 5. Perform root-cause analysis to determine underlying causes of process variation for continuous improvement.					PO1.6 ME4.6				5.1.1 5.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD – External Dependencies													
EXD:SG1 Identify and Prioritize External Dependencies													
EXD:SG1.SP1 Identify External Dependencies Subpractices 1. Establish a process for creating and maintaining the list of external dependencies and entities. 2. Establish a set of information that is collected and stored to define each external dependency and the responsible external entity. 3. Review the organization's asset inventory to ensure that any external entities that possess, develop, control, operate, or otherwise influence high-value assets are identified as external dependencies.		6.1 6.4 7.7.2 8.5.8	SAM:SP1.2	SAM:SP1.2 SD:SP1.1	PO8.4 AI5.1 DS2.1	Appendix E: Interde-pendencies	6.1.2 6.1.3 7.3.3	6.7.2 5.5.1 5.5.2	6.1.6 6.1.7 10.2.1			5.2.1 5.2.4 6.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG1.SP1 Identify External Dependencies Subpractices (continued) 4. Review the organization's list of services to identify services that are subject to external dependencies; add any such dependencies to the list of external dependencies. 5. Review supplier and customer databases to identify additional external dependencies. 6. Review current contracts and SLAs to identify additional external dependencies. 7. Update the external dependency list on a regular basis.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG1.SP2 Prioritize External Dependencies Subpractices 1. Establish prioritization criteria and scheme for external dependencies. 2. Apply the prioritization criteria to the list of external dependencies to produce a prioritized list. 3. Periodically validate and update the prioritization criteria and scheme based on changes to the operational environment. 4. Periodically update the prioritized list of external dependencies based on changes in the prioritization criteria and scheme, the operating environment, or the list of external dependencies. 5. Perform affinity analyses to inform dependency prioritization and risk identification.		7.7.2											

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG2 Manage Risks Due to External Dependencies													
EXD:SG2.SP1 Identify and Assess Risks Due to External Dependencies Subpractices 1. Determine the scope of risk assessment. 2. Identify risks due to external dependencies. 3. Analyze risks due to external dependencies. 4. Categorize and prioritize risks. 5. Assign a risk disposition to each identified risk.		4.5			DS2.3			5.5.1 5.6.5 6.7.3	6.2.1 6.2.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG2.SP2 Mitigate Risks Due to External Dependencies		4.5			DS2.3			5.5.1 5.5.2 5.6.5 6.7.3	6.2.1 6.2.2				
Subpractices 1. Develop risk mitigation strategies and plans for all risks due to external dependencies that have a "mitigation" or "control" disposition. 2. Validate the risk mitigation plans by comparing them to existing strategies for protecting and sustaining external dependencies. 3. Identify the person or group responsible for each risk mitigation plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan. 4. Monitor and manage residual risk. 5. Implement the risk mitigation plans and provide a method for monitoring their effectiveness.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG2.SP2 Mitigate Risks Due to External Dependencies Subpractices (continued) 6. Monitor risk status on a regular basis to ensure that the risk, its mitigation strategy, and its plan do not pose additional threat to the organization.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG3 Establish Formal Relationships													
EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies Subpractices 1. Establish a list of enterprise-level specifications that apply to external dependencies and entities. 2. Include specifications to adhere to relevant policies, standards, and guidelines (particularly those that support or affect the resilience of the organization or its operations) in the list of enterprise specifications for external dependencies and entities. 3. Include relevant compliance and regulatory requirements in the list of enterprise specifications for external dependencies and entities.				SD:SP2.1	AI5.4 DS1.1	Risk Man-agement	6.1.2 6.1.3	5.6 5.8.1 5.8.2 6.3.4 6.3.9 7				6.2.2 6.2.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG3.SP1 Establish Enterprise Specifications for External Dependencies Subpractices (continued) 4. Include the enterprise specifications for external dependencies and entities in contract and agreement templates as appropriate. 5. Review and update the enterprise specifications for external dependencies and entities on a regular basis. 6. Ensure that changes are initiated to agreements with external entities when the enterprise specifications change.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG3.SP2 Establish Resilience Specifications for External Dependencies				SD:SP2.1 SD:SP2.3	AI5.4 DS1.1	Risk Man-agement		5.5.3 5.5.4 5.5.5 5.6 5.8.1 5.8.2 6.3.9 6.7.3 6.8.2 6.14.5 7	6.2.3 10.2.1 12.5.5				
Subpractices 1. For each external dependency, establish a list of resilience specifications that apply to the responsible external entity. 2. Include specific characteristics of the external entity that are required. 3. Include resilience requirements for assets that will be developed, provided, or maintained by external entities. 4. Include required behaviors, standards of performance, and service levels that are required of the external entity. 5. Periodically review and update resilience specifications for external dependencies and entities as conditions warrant.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG3.SP3 Evaluate and Select External Entities		4.5			AI5.3			5.6.6 6.7.2 6.8.2 6.14.5 7 8.4 8.5					
Subpractices 1. Establish a selection process for external entities that includes consideration of applicable specifications. 2. Establish external entity selection criteria. 3. Include the resilience specifications for external entities in RFPs, other solicitations of interest, and other documents or processes that are designed to identify and/or qualify candidate external entities. 4. Evaluate external entities based on their abilities to meet the resilience specifications and in accordance with the established selection criteria. 5. Perform due diligence on candidate external entities. Approve allocation of funding to resilience engineering program and process activities.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG3.SP3 Evaluate and Select External Entities Subpractices (continued) 6. Select external entities and document the selection and decision rationale. 7. If any resilience specifications are unmet by the selected external entity, revise the selection criteria to adjust the specifications or treat the unmet specifications as identified risks in EXD:SG2.SP1.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG3.SP4 Formalize Relationships		5.5	SAM:SP1.3 SAM:SP2.1	SAM:SP1.3 SAM:SP2.1 SD:SP1.2	AI5.4 DS1.3 DS1.4 DS2.2		6.1.2 6.1.3 7.2.1 7.3.1 7.3.2 7.3.3	5.5.3 5.5.4 5.5.5 5.6 5.8.1 5.8.2 6.3.5 6.3.7 7.6.2 7.6.4	6.2.3 10.8.2			6.2.2 6.2.3	
Subpractices 1. Select an agreement type that best fits the performance standards required by the organization and that is enforceable if problems arise. 2. Properly document the agreement terms, conditions, specifications, and other provisions. 3. Ensure that the organization and the external entity agree to all agreement provisions and specifications before executing the agreement. 4. Update the agreement as required throughout the duration of the agreement according to provisions established in the agreement.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG4 Manage External Entity Performance													
EXD:SG4.SP1 Monitor External Entity Performance Subpractices 1. Establish procedures and responsibility for monitoring external entity performance and inspecting external entity deliverables. 2. Meet periodically with external entity representatives to review the result of monitoring activities, the specifications in the agreement, and any changes in either the organization or the external entity that might impact performance under the agreement. 3. Evaluate any deviations in the performance of the external entity from the established specifications to determine the risk to the organization's operation and to inform the selection of corrective actions.		4.5	SAM:SP2.2 SAM:SP2.3 SAM:SP2.4	SAM:SP2.2 SAM:SP2.3 SAM:SP2.4 SD:SP3.3	AI4.2 DS1.5 DS1.6 DS2.4 ME2.6		6.1.3 7.2.1 7.2.2 7.2.3 7.3.1 7.3.3	5.6.4 5.6.5 6.8.2 7.5.10 7.6.1 7.6.3 7.6.7 7.10.3 7.16.3 9.3.1	10.2.2 12.5.5				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
EXD:SG4.SP2 Correct External Entity Performance Subpractices 1. Evaluate alternative corrective actions to select the optimal corrective action. 2. Communicate with the external entity to review selected corrective actions. 3. Implement selected corrective actions. 4. Monitor as appropriate to ensure that issues are remedied in a timely manner. 5. Update the agreement with the external entity as required.			SAM:SP2.2 SAM:SP2.3 SAM:SP2.4	SAM:SP2.2 SAM:SP2.3 SAM:SP2.4 SD:SP3.3	AI4.2 DS1.6 DS2.4 ME2.7		6.1.3 7.2.1 7.2.2 7.3.1	5.6.5 6.8.2	10.2.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM – Financial Resource Management													
FRM:SG1 Establish Financial Commitment													
FRM:SG1.SP1 Commit Funding for Operational Resilience Management Subpractices 1. Develop the business case for the operational resilience management program and process. 2. Establish operational resilience management program and process funding as a regular part of the organization's strategic plan budgeting (capital and expense) exercise. 3. Define the sources of funds that will be used to fund the operational resilience management program and process activities.					DS6.1		3.1 4.1.4 6.4.2					4.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG1.SP1 Commit Funding for Operational Resilience Management Subpractices (continued) 4. Approve allocation of funding to operational resilience management program and process activities.													
FRM:SG1.SP2 Establish Structure to Support Financial Management Subpractices 1. Establish resilience accounting policies and procedures. 2. Establish resilience accounts, cost strings, and budgeting processes. 3. Establish tools and techniques for resilience financial management. 4. Assign responsibility and accountability for resilience budgeting, funding, and accounting activities.					PO5.1		6.4.1					4.7.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG2 Perform Financial Planning													
FRM:SG2.SP1 Define Funding Needs Subpractices 1. Collect historical data that will be used as the basis for developing funding requirements. 2. Determine and document resilience funding requirements. 3. Validate funding assumptions through detailed analysis of resilience requirements.			PP:SP1.4		PO5.4		6.4.2						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG2.SP2 Establish Resilience Budgets Subpractices 1. Determine the budgets available for the resilience program. 2. Establish a budgeting methodology and process for resilience. 3. Develop the operational-level resilience budgets. 4. Develop the enterprise-level resilience budgets. 5. Assign authority and accountability for developing and managing the budgets. 6. Review budgets on a regular basis and update as necessary. 7. Tie performance measures to the resilience budgets.			PP:SP2.1		PO5.3		6.4.2 6.4.3					4.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG2.SP3 Resolve Funding Gaps Subpractices 1. Perform gap analysis between resilience funding needs and established budgets. 2. Identify budget shortfalls. 3. Identify risks related to budget shortfalls. 4. Develop and document decisions to resolve potential issues, concerns, and risks that result from funding gaps.					PO5.3		6.4.3						
FRM:SG3 Fund Resilience Activities													
FRM:SG3.SP1 Fund Resilience Activities Subpractices 1. Develop policies and procedures for accessing resilience-budgeted funds. 2. Develop a process for addressing off-cycle or off-budget funds requests and approvals.							6.4.3					4.4 4.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG4 Account for Resilience Activities													
FRM:SG4.SP1 Track and Document Costs Subpractices 1. Develop and implement a means for collecting and tracking costs. 2. Collect financial data on the costs related to providing resilience services. 3. Calculate variances between budgeted costs and actual costs. 4. Identify and document major budget variances. 5. Analyze budgets on a regular basis to determine potential period shortfalls or unspent items. 6. Revise budgets based on actual data if necessary.					DS6.2 DS6.4 PO5.4		4.1.4 6.4.2 6.4.3 6.4.4					4.4 4.7.5	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG4.SP2 Perform Cost and Performance Analysis Subpractices 1. Perform analysis on budget variances and document explanations for the variances. 2. Develop plans for reducing or eliminating variances. 3. Calculate the true cost of providing resilience services (COR). 4. Report financial exceptions.					DS6.3 DS6.4 PO5.4		4.1.4 6.4.2 6.4.3						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG5 Optimize Resilience Expenditures and Investments													
FRM:SG5.SP1 Optimize Resilience Expenditures Subpractices 1. Establish scope of optimization calculations and examination. 2. Perform optimization calculations on high-value assets and/or services. 3. Identify opportunities for optimization. 4. Revise strategies to provide optimal operational resilience.					PO5.4 PO5.5		6.4.4						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG5.SP2 Determine Return on Resilience Investments					PO5.5	BCP Pro-cess	6.4.4					5.5	
Subpractices 1. Establish and collect objective and quantifiable variables to include in the RORI calculation. 2. Establish the scope of the calculation. 3. Perform the RORI calculation. 4. Analyze results of RORI calculation. 5. Develop and implement strategies to improve RORI.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
FRM:SG5.SP3 Identify Cost Recovery Opportunities Subpractices 1. Determine areas where resilience costs can be assigned to and included in the production costs for services and products. 2. Determine appropriate level of resilience cost charge-backs. 3. Include resilience costs in the determination of standard costs for services and products.					PO5.5								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM – Human Resource Management													
HRM:SG1 Establish Resource Needs													
HRM:SG1.SP1 Establish Baseline Competencies Subpractices 1. Establish and document baseline competencies necessary to meet the needs of the organization's operational resilience management system. 2. Create or update job descriptions to reflect base competencies.					PO4.12 PO7.1 PO7.2		3.3.1	8.3	8.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG1.SP2 Inventory Skills and Identify Gaps Subpractices 1. Develop a skills inventory, particularly relevant to resilience skills. 2. Compare baseline competencies to the current skills inventory. 3. Identify skill gaps and deficiencies. 4. Develop processes to keep the skills inventory current and for performing regular comparison to baseline competencies.					PO4.12 PO7.2 PO7.3		3.3.1 3.3.2 3.3.3		8.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG1.SP3 Address Skill Deficiencies Subpractices 1. Develop strategy for addressing skill gaps. 2. Update job descriptions to incorporate missing skills as necessary. 3. Develop job requisitions for unfilled positions. 4. Develop training plans for skills that can be obtained by existing staff. 5. Refer resulting risks to the risk management process for disposition.			PP:SP2.5		PO7.2 PO7.3 PO7.4		3.3.1 3.3.2 3.3.3		8.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG2 Manage Staff Acquisition													
HRM:SG2.SP1 Verify Suitability of Candidate Staff Subpractices 1. Establish baseline verification criteria that apply to all positions in the organization. 2. Establish job-specific verification criteria that apply to vital positions. 3. Establish verification program and procedures. 4. Review and revise verification criteria and program as required.					PO4.12 PO7.6		3.3.2 3.3.3	5.5.5 5.6.6 5.9.1 6.3.2 6.3.4 6.3.9 6.14.4 8.3	8.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG2.SP2 Establish Terms and Conditions of Employment Subpractices 1. Establish baseline terms and conditions of employment that apply to all positions in the organization. 2. Ensure that terms and conditions are clearly documented in job descriptions. 3. Execute agreements as necessary to enforce employment terms and conditions.					PO4.14 PO7.3			5.5.5 5.6.6	8.1.1 8.1.2 8.1.3 8.2.1 9.2.7 11.2.3 11.3.1 15.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG3 Manage Staff Performance													
HRM:SG3.SP1 Establish Resilience as a Job Responsibility Subpractices 1. Insert resilience obligations into job descriptions. 2. Ensure that job descriptions and resilience requirements are communicated to candidate staff prior to employment.					PO4.14	Board and Senior Manage-ment Re-sponsibility	3.3.1	6.3.4	6.1.3 8.1.1 8.2.1 11.2.3 11.3.1 13.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG3.SP2 Establish Resilience Performance Goals and Objectives Subpractices 1. Review resilience obligations, roles, and responsibilities of the position as the basis for establishing resilience goals and objectives. 2. Formalize and establish resilience goals and objectives in writing. 3. Ensure that the staff members understand resilience goals and objectives.								6.3.9	6.1.3 8.2.1 11.2.3 11.3.1 13.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG3.SP3 Measure and Assess Performance Subpractices 1. Measure performance against resilience goals and objectives. 2. Conduct performance evaluations. 3. Acknowledge performance achievements as appropriate. 4. Identify improvement opportunities and take corrective actions as necessary. 5. Revise goals and objectives as needed.					PO7.7		3.3.1 3.3.3	7.5.8					
HRM:SG3.SP4 Establish Disciplinary Process Subpractices 1. Establish an investigation process. 2. Establish a disciplinary process. 3. Revise the disciplinary process as needed.									8.2.3 15.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG4 Manage Changes to Employment Status													
HRM:SG4.SP1 Manage Impact of Position Changes Subpractices 1. Establish and execute an exit interview process. 2. Develop a plan for reassignment of roles and responsibilities. 3. Reassign resilience roles and functions upon a staff member's departure from a position. 4. Review and confirm understanding of confidentiality agreements and obtain assurances for compliance.					PO7.8		3.3.2	5.6.6 6.3.4	8.3.1 15.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
HRM:SG4.SP2 Manage Access to Assets Subpractices 1. Secure the return of all organizational assets, property, and information upon a staff member's departure. 2. Inventory all organizational assets, property, and information in possession of staff upon position changes, and make necessary adjustments. 3. Discontinue all access to organizational assets upon termination or position changes.					PO7.8			6.3.4	8.3.2 8.3.3 15.1.2				
HRM:SG4.SP3 Manage Involuntary Terminations Subpractices 1. Establish criteria for determining potential risks related to involuntary terminations. 2. Establish procedures for managing involuntary terminations.					PO7.8		3.3.2	6.3.4	8.3.1 8.3.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ID – Identity Management													
ID:SG1 Establish Identities													
ID:SG1.SP1 Create Identities Subpractices 1. Establish an identity profile for persons, objects, and entities.					DS5.3		6.4.8	5.7.1 6.3.2	10.9.1 11.1.1 11.2.1,2 11.5.2,4 11.6.1				
ID:SG1.SP2 Establish Identity Community Subpractices 1. Create and maintain an identity repository. 2. Deposit identity profiles as they are created into the identity repository. 3. Establish access controls to ensure protection over identity information.					DS5.3			5.7.1 6.3.2 6.4.8	10.9.1 11.2.1,2 11.2.3 11.3.1 11.4.1,2,3 11.5.4 12.4.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ID:SG1.SP3 Assign Roles to Identities Subpractices 1. Develop, authorize, and justify roles. 2. Assign roles to identities.					DS5.3			6.3.2 6.4.8	10.9.1 11.2.1 11.2.2 11.5.4				
ID:SG2 Manage Identities													
ID:SG2.SP1 Monitor and Manage Identity Changes Subpractices 1. Establish organizational criteria that may signify changes in the identity community. 2. Monitor for and manage changes to identity community.								6.3.4	11.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ID:SG2.SP2 Periodically Review and Maintain Identities Subpractices 1. Establish regular review cycle and process. 2. Perform review of identity community. 3. Identify inconsistencies in the identity community.					DS5.4			6.3.4	11.2.1 11.2.4				
ID:SG2.SP3 Correct Inconsistencies Subpractices 1. Develop corrective actions to address inconsistencies in identity profiles. 2. Correct identity profiles as required. 3. Document disposition for inconsistencies that will not result in changes or corrections. 4. Update status on corrective actions.					DS5.4			6.3.4	11.2.1 11.2.4				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
ID:SG2.SP4 Deprovision Identities Subpractices 1. Obtain written approval from line of business and organizational unit managers, asset owners, and human resources staff for deprovisioning identities. 2. Identify and trace access privileges associated with the identity's roles. 3. Deprovision identities as required.					DS5.3 DS5.4 PO7.8			6.3.4	11.2.1 11.2.4				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC – Incident Management and Control													
IMC:SG1 Establish the Incident Management and Control Process													
IMC:SG1.SP1 Plan for Incident Management Subpractices 1. Establish the incident management plan content. 2. Establish commitments to the plan. 3. Revise the plan and commitments as necessary.	4.4.7	5.5 7.8 7.9 8.2 8.3 8.4 8.5		IRP:SP1.1 IRP:SP1.2	PO10.9	Risk Management Other Policies, Standards, and Processes Appendix D: Pandemic Planning	6.6.6 8.2.1	5.3.4 5.7.5 6.10.5				5.1.1 5.2 5.7.1 6.4.2 6.9.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG1.SP2 Assign Staff to the Incident Management Plan Subpractices 1. Develop detailed job descriptions for each role/responsibility detailed in the incident management plan. 2. Establish a list of candidate and skilled staff to fill each role/responsibility in the incident management plan. 3. Assign staff to incident management roles and responsibilities. 4. Ensure that organizational training is provided to incident staff respective to their specific incident management job responsibilities.		7.8 8.3.3 8.3.5 8.3.6 8.4 8.5.2 8.5.3 8.5.4 8.5.5 8.5.6		IRP:SP1.1 IRP:SP1.2		Other Policies, Standards, and Pro-cesses	6.1.2	5.3.4				5.2.2 5.2.3 5.2.4 5.2.5 6.5.1 6.9.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG2 Detect Events													
IMC:SG2.SP1 Detect and Report Events Subpractices 1. Define the methods of event detection and reporting. 2. Develop and communicate descriptions of event detection and reporting roles and responsibilities. 3. Assign the roles of event detection and reporting to appropriate staff throughout the organization. 4. Establish a process for event reporting. Document events as they are detected on an event report. 5. Submit event reports to appropriate management staff per the organization's event reporting process.				IRP:SP2.1	DS8.1 DS10.1 PO9.3		6.6.6 8.1.2 8.2.1 8.3.2	5.7.5 6.3.11 6.4.6	6.2.2 10.4.1 10.10.1 10.10.2 12.5.4 13.1.1 13.2.1			6.4.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG2.SP1 Detect and Report Events Subpractices (continued) 6. Provide training and awareness for managers and users of technology assets (systems, networks, etc.) to identify anomalies and to report these anomalies to the service desk or other authorized source for investigation and resolution.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG2.SP2 Log and Track Events Subpractices 1. Develop and implement an incident management knowledgebase that allows for the entry of event reports (and the tracking of declared incidents) through all phases of their life cycle. 2. Enter event reports to the incident management knowledgebase as they are received. 3. Establish and distribute standard reports that provide status information on events as they move through the life cycle.				IRP:SP2.1	DS8.1 DS8.2 DS10.2		8.1.2 8.2.1 8.3.2	5.7.5.1	10.10.1 10.10.2 10.10.5 12.5.4 13.1.1 13.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG2.SP3 Collect, Document, and Preserve Event Evidence Subpractices 1. Identify relevant rules, laws, regulations, and policies for which incident evidence may be required. 2. Develop and communicate consistent guidelines and standards for collection, documentation, and preservation of evidence for events/incidents. 3. Document events and related evidence information in the incident management knowledgebase where practical.				IRP:SP2.1				5.7.5.1	13.1.1 13.2.1 13.2.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG2.SP4 Analyze and Triage Events				IRP:SP2.2		Risk Assessment		5.7.5.1					
Subpractices 1. Assign a category to events from standard category definitions. 2. Perform correlation analysis on event reports to determine if there is affinity between two or more events. 3. Prioritize events. 4. Assign a disposition to events. 5. Escalate events if they require additional analysis. 6. Update the knowledgebase with information gathered in the triage process and the event disposition. 7. Assign events that have not been assigned a "closed" status for further analysis and resolution. 8. Periodically review the incident knowledgebase for events that have not been closed for which there is no disposition.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG3 Declare Incidents													
IMC:SG3.SP1 Define and Maintain Incident Declaration Criteria Subpractices 1. Establish incident declaration criteria for use in guiding when to declare an incident. 2. Distribute incident declaration criteria to all sources and relevant staff who may need to declare an incident. 3. Update incident declaration criteria as required based on experience in past declarations.		8.3.4			DS5.6 DS10.1	Risk Management Other Policies, Standards, and Processes						5.1.3 5.4.2 6.9.5	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG3.SP2 Analyze Incidents Subpractices 1. Establish and communicate a standardized and consistent incident analysis approach and structure. 2. Identify relevant analysis tools, techniques, and activities that the organization will use to analyze incidents and develop an appropriate response. 3. Analyze open event reports and previously declared incidents. 4. Document analysis on an incident analysis report.				IRP:SP2.2 IRP:SP3.1		Risk Man-agement	8.1.2 8.2.1	5.7.5.1	13.2.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG4 Respond to and Recover from Incidents													
IMC:SG4.SP1 Escalate Incidents Subpractices 1. Develop incident escalation criteria. 2. Develop incident escalation procedures. 3. Communicate incident escalation criteria and procedures to those who have responsibility for identifying and escalating incidents. 4. Escalate incidents to appropriate stakeholders for resolution.		8.5.6			DS8.3	Risk Man-agement	8.2.1	5.7.5.1 6.3.9	6.1.6 13.1.1 13.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG4.SP2 Develop Incident Response		8.2 8.3 8.4		IRP:SP2.3 IRP:SP2.4 IRP:SP2.6 IRP:SP3.2	DS8.3 DS3.4	Risk Man-agement	6.1.2 8.1.2 8.2.1 8.2.2	5.7.5.1 5.8.1 5.8.2	6.1.6 13.1.1 13.2.1			5.7.1 6.4.2 6.4.3 6.4.5	
Subpractices 1. Develop an incident response strategy and plan to limit incident effect and to repair incident damage. 2. Identify staff who are responsible for coordinating incident response (across all potential types of incidents) and ensure they have the authority and responsibility to act. 3. Update the incident knowledgebase with information about the incident response strategy and plan.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG4.SP3 Communicate Incidents Subpractices 1. Identify relevant stakeholders that may have a vested interest or vital role in communications about an organizational incident. 2. Identify the appropriate communications protocols and channels (media and message) for each type of stakeholder. 3. Develop and implement an organizational incident management communications plan. 4. Identify and obtain commitment from staff who are required to carry out the incident communications plan. 5. Identify and train staff resources responsible for incident communication and provide general guidelines for incident response and other personnel for appropriate communication of incident information.		7.9 8.5.5 8.5.6			DS5.6 DS8.3	Risk Man-agement	8.2.1	6.3.11	13.1.1 13.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG4.SP4 Close Incidents Subpractices 1. Establish criteria for incident closure. 2. Define and assign responsibility for incident closure. 3. Update the knowledgebase to indicate that an incident has been closed. 4. Track incidents that have been open for an extended period of time without closure and resolve.				IRP:SP2.5	DS8.4 DS10.3 DS10.4	Risk Management	8.1.2 8.2.1		13.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG5 Establish Incident Learning													
IMC:SG5.SP1 Perform Post-Incident Review Subpractices 1. Establish and implement a formal post-incident response activity and require it as part of closing an incident. 2. Assign responsibility for post-incident review activities to appropriate personnel and ensure they are properly trained. 3. Identify root-cause analysis tools and techniques and ensure all personnel who participate in analysis are trained in their use. 4. Prepare a post-incident analysis report. 5. Document the results of post-incident root cause analysis in the knowledgebase so that this information is available for use in other processes (e.g. problem management).					DS8.5 DS10.2	Risk Man-agement	8.1.2 8.2.1 8.2.2 8.3.1 8.3.8 8.3.9	5.7.5.1	13.2.2			6.4.5 8.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG5.SP2 Integrate with the Problem Management Process Subpractices 1. Establish a problem management system to ensure that all operational events that are not part of standard operation (incidents, problems, and errors) are recorded, analyzed, and resolved in a timely manner. 2. Document problem reports that arise from incident management and deliver these reports to the problem management process. 3. Periodically review problem reports and their status to determine their impact on future incident detection and analysis. 4. Update the incident knowledgebase with information gathered in the problem management process.					DS8.5 DS10.1 DS10.4	Risk Management Other Policies, Standards, and Processes	8.1.2 8.2.1 8.3.1 8.3.2 8.3.8 8.3.9	5.7.5.2	13.2.2			6.4.5	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG5.SP3 Translate Experience to Strategy Subpractices 1. Review knowledgebase information and update the following areas accordingly: • Protection strategies and controls for assets involved in the incident • Continuity plans and sustainability strategies for assets involved in the incident • Information security and other organizational policies that need to reflect new standards, procedures, and guidelines based on what is learned in the incident handling • Training for personnel on information security, business continuity, and IT operations 2. Review incident management and control processes and update for any perceived deficiencies or omissions.		9.5.1 9.5.2 9.5.3 9.5.4 9.5.5 9.5.6				Risk As-sessment	8.2.2 8.3.1	5.7.5	6.1.2 13.2.2			8.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
IMC:SG5.SP3 Translate Experience to Strategy Subpractices (continued) 3. Update resilience requirements for assets and services based on what is learned in the incident management process. 4. Quantify and monitor the types, volumes, and costs of incidents.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM – Knowledge and Information Management													
KIM:SG1 Establish and Prioritize Information Assets													
KIM:SG1.SP1 Prioritize Information Assets Subpractices 1. Compile a list of high-value information assets from the organization's information asset inventory. 2. Periodically validate and update the list of high-value information assets based on operational and organizational environment changes.		6.4 7.6					6.6.2		7.2.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG1.SP2 Categorize Information Assets Subpractices 1. Develop an information asset categorization scheme. 2. Assign responsibility for the assignment of sensitivity categorization levels to information assets. 3. Assign sensitivity categorization levels to information assets. 4. Establish policies for proper handling of information assets according to the sensitivity categorization scheme. 5. Establish policies and procedure for proper labeling of each category of information asset.					PO2.3 PO4.9		6.6.2		7.2.1 7.2.2 10.7.3 10.10.3 15.1.2 15.3.1 15.3.2			4.8.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG2 Protect Information Assets													
KIM:SG2.SP1 Assign Resilience Requirements to Information Assets Subpractices 1. Assign resilience requirements to high-value information assets. 2. Document the requirements (if they are currently not documented) and include in the asset definition.		6.4 7.6			PO2.4 DS4.8 DS5.7 DS5.11 DS11.1 DS11.6 DS13.4	Appendix G: BCP Components		5.3.3 5.7.1 5.7.4 6.4.11 6.4.12 6.4.14	6.2.2 7.1.3 10.7.4 10.8.1 10.9.2 12.3.1			4.4 5.5.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG2.SP2 Establish and Implement Controls Subpractices 1. Establish and implement administrative controls for information assets. 2. Establish and implement technical controls for information assets. 3. Establish and implement physical controls for information assets. 4. Monitor the effectiveness of administrative, technical, and physical controls, and identify deficiencies that must be resolved.					PO2.4 DS5.7 DS11.1 DS11.6 DS13.4			5.7.1 5.7.4 6.3.3 6.3.5 6.3.6 6.3.7 6.4.11 6.4.12 6.4.14	6.1.5 6.2.2 7.1.3 9.2.5,7 10.1.1,3,4 10.4.1,2 10.6.1,2 10.7,8 10.9.2,3 10.10.1,2 10.10.3,6 11.2-11.7 12.2 12.4.1,2,3 12.5.1,2,4 15.1.3,4,5				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG3 Manage Information Asset Risk													
KIM:SG3.SP1 Identify and Assess Information Asset Risk Subpractices 1. Determine the scope of the risk assessment for information assets. 2. Identify risks to information assets. 3. Analyze risks to information assets. 4. Categorize and prioritize risks to information assets. 5. Assign a risk disposition to each information asset risk. 6. Monitor the risk and the risk strategy on a regular basis to ensure that it does not pose additional threat to the organization. 7. Develop a strategy for those risks that the organization decides to mitigate.		7.3	PP:SP2.2		PO9.1 PO9.4	Risk Man-agement			10.10.2 11.2-7 12.2.3 15.1.3			5.6.1 5.6.2 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG3.SP2 Mitigate Information Asset Risk Subpractices 1. Develop and implement risk mitigation strategies for all risks that have a "mitigation" or "control" disposition. 2. Validate the risk mitigation plans by comparing them to existing protection and sustainability strategies. 3. Identify the person or group responsible for each risk mitigation plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan. 4. Address residual risk. 5. Implement the risk mitigation plans and provide a method to monitor the effectiveness of these plans. 6. Monitor risks status. 7. Collect performance measures on the risk management process.		7.3			PO9.4 PO9.5	Risk Management		6.4.11 6.4.12 6.4.14	11.2-7 12.2.3 15.1.3			5.6.1 5.6.2 5.6.3 5.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG4 Manage Information Asset Confidentiality and Privacy													
KIM:SG4.SP1 Encrypt High-Value Information Subpractices 1. Establish an organizational policy and program addressing the proper use of encryption and cryptographic means for protecting information assets. 2. Establish a list of acceptable cryptographic technologies preferred by the organization. 3. Encrypt information assets based on policy and information asset categorization.					DS5.8 DS5.11			5.7.2 5.7.4	6.1.5 10.6.1 10.7.4 10.8.1 10.8.2 10.8.4 10.9.2 12.2.3 12.3 15.1.4 15.1.6				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG4.SP2 Control Access to Information Assets Subpractices 1. Identify the information assets to which access must be controlled. 2. Develop and implement access controls to satisfy confidentiality and privacy-related resilience requirements. 3. Manage access controls on an ongoing basis to ensure continued satisfaction of confidentiality and privacy-related resilience requirements.					DS5.10 DS5.11			5.7.2 5.7.4 7.4.3	6.1.5 10.1.4 10.6.1 10.7.4 10.8.4,5 10.9.2 10.10.1 10.10.3 12.2.3 15.1.3,4 15.3.1,2			4.8.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG4.SP3 Control Information Asset Disposition Subpractices 1. Develop and implement guidelines for the appropriate disposition of information assets. 2. Communicate these guidelines to all personnel who are responsible for the resilience of information assets.					DS11.4			6.4.14	6.1.5 9.2.6 10.7.1 10.7.2 15.1.3 15.1.4			4.8.2 5.8.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG5 Manage Information Asset Integrity													
KIM:SG5.SP1 Control Modification of Information Assets Subpractices 1. Establish organizationally acceptable tools, techniques, and methods for modifying information assets. 2. Identify and document personnel who are authorized to modify information assets, relative to the asset's integrity requirements. 3. Implement tools, techniques, and methods to monitor and log modification activity on high-value information assets. 4. Perform periodic audits of information asset modification logs and identify and address anomalies.					PO2.4 DS5.11 DS5.10			5.7.4	10.1.1 10.1.4 10.7.4 10.9.2 10.9.3 10.10.3 12.2.3 12.4.2 12.4.3 15.1.3			4.8.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG5.SP2 Manage Information Asset Configuration Subpractices 1. Establish information asset baseline to serve as the foundation for information asset change control. 2. Develop and implement configuration control policies, procedures, and techniques. 3. Review configuration control logs and identify anomalies.					PO2.4 DS5.10			5.7.4	10.1.1 10.1.4 10.9.2 10.9.3 12.2.3 12.5.2 15.1.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG5.SP3 Verify Validity of Information Subpractices 1. Establish requirements for the inclusion of data validation controls in services and related systems. 2. Perform regular review of information asset output from processes. 3. Periodically verify (through monitoring and auditing) that changes are valid and authorized.					PO2.4 DS5.10 DS5.11 DS11.1				10.1.1 10.9.2 10.9.3 12.2 12.5.1 12.5.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG6 Manage Information Asset Availability													
KIM:SG6.SP1 Perform Information Duplication and Retention Subpractices 1. Develop information asset backup and retention procedures. 2. Backup and store information assets as prescribed and according to their availability requirements. 3. Periodically test the organization's backup and storage procedures and guidelines to ensure continued validity as operational conditions change.		7.3 7.6			PO2.4 DS4.9 DS11.2 DS11.3 DS11.5 AI7.5		6.3.4	6.9.3	10.1.1 10.5.1 15.1.3			4.8.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
KIM:SG6.SP2 Manage Organizational Knowledge		7.3 7.6			PO2.4 PO7.5			6.9.3 7.4.2	15.1.3			4.8.2	
Subpractices 1. Identify vital staff who may have institutional knowledge. 2. Identify information assets that may be in intangible forms. 3. Document information assets as necessary. 4. Develop and implement procedures for regular identification, capture, and revision of institutional knowledge.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA – Measurement and Analysis													
MA:SG1 Align Measurement and Analysis Activities													
MA:SG1.SP1 Establish Measurement Objectives Subpractices 1. Document information needs and objectives. 2. Prioritize information needs and objectives. 3. Document, review, and update measurement objectives. 4. Provide feedback for refining and clarifying information needs and objectives as necessary. 5. Maintain traceability of the measurement objective to the identified information needs and objectives.		6.2	MA:SP1.1	CAM:SP1.2 MA:SP1.1	DS8.5 PO8.6 PO10.13		4.3	9.3.1				4.6	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA:SG1.SP2 Specify Measures Subpractices 1. Identify candidate measures based on documented measurement objectives. 2. Identify existing measures that already address the measurement objectives. 3. Specify operational definitions for the measures. 4. Prioritize, review, and update measures.		6.2	MA:SP1.2 QPM:SP2.1	CAM:SP1.2 MA:SP1.2 QPM:SP2.1	DS8.5 PO10.13			9.3.2 4.3				4.6	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA:SG1.SP3 Specify Data Collection and Storage Procedures Subpractices 1. Identify existing sources of data that are generated from current processes or transactions. 2. Identify measures for which data is needed but is not currently available. 3. Specify how to collect and store the data for each required measure. 4. Create data collection mechanisms and process guidance. 5. Support automatic collection of the data where appropriate and feasible. 6. Prioritize, review, and update data collection and storage procedures. 7. Update measures and measurement objectives as necessary.			MA:SP1.3	CAM:SP1.2 MA:SP1.3 OID:SP1.2 PPQA:SP2.2									

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA:SG1.SP4 Specify Analysis Procedures Subpractices 1. Specify and prioritize the analyses that will be conducted and the reports that will be prepared. 2. Select appropriate data analysis methods and tools. 3. Specify administrative procedures for analyzing the data and communicating the results. 4. Review and update the proposed content and format of the specified analyses and reports. 5. Update measures and measurement objectives as necessary. 6. Specify criteria for evaluating the utility of the analysis results and for evaluating the conduct of the measurement and analysis activities.			MA:SP1.4 QPM:SP2.1	CAM:SP1.2 MA:SP1.4 OID:SP1.2 QPM:SP2.1	PO8.6 PO10.13								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA:SG2 Provide Measurement Results													
MA:SG2.SP1 Collect Measurement Data Subpractices 1. Obtain the data for base measures. 2. Generate the data for derived measures. 3. Perform data integrity checks as close to the source of the data as possible.			MA:SP2.1	CAM:SP2.1 CAM:SP2.2 MA:SP2.1	DS8.5 PO10.13		4.3	9.1					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA:SG2.SP2 Analyze Measurement Data Subpractices 1. Conduct initial analyses, interpret the results, and draw preliminary conclusions. 2. Conduct additional measurements and analysis as necessary, and prepare results for presentation. 3. Review the initial results with relevant stakeholders. 4. Refine criteria for future analyses.			MA:SP2.2 PQA:SP1.2 QPM:SP2.2	CAM:SP2.1 CAM:SP2.2 MA:SP2.2 OID:SP1.2 OID:SP2.3 PPQA:SP1.2 QPM:SP2.2	DS8.5 PO8.6 PO10.13		4.3						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MA:SG2.SP3 Store Data and Results Subpractices 1. Review the data to ensure its completeness, integrity, accuracy, and currency. 2. Store the data according to the data storage procedures. 3. Make the stored contents available for use only by appropriate groups and staff. 4. Prevent the stored information from being used inappropriately.			MA:SP2.3 QPM:SP2.3 QPM:SP2.4	MA:SP2.3 QPM:SP2.3	PO8.6								
MA:SG2.SP4 Communicate Results Subpractices 1. Keep relevant stakeholders apprised of measurement results on a timely basis. 2. Assist relevant stakeholders in understanding the results.			MA:SP2.4 PPQA:SP2.1	MA:SP2.4 PPQA:SP2.1	PO8.6								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MON – Monitoring													
MON:SG1 Establish and Maintain a Monitoring Program													
MON:SG1.SP1 Establish a Monitoring Program Subpractices 1. Establish the plan and scope for a resilience monitoring program. 2. Establish commitments to the plan. 3. Revise the plan and commitments as necessary.	4.5.1			PMC:SP1	ME1.1 ME1.2			6.4.4 6.4.5.1 6.14.10 7.5.6				5.4.2 5.6.4	
MON:SG1.SP2 Identify Stakeholders Subpractices 1. Identify stakeholders of the monitoring process. 2. Develop and document a stakeholder involvement plan.				PMC:SP1	AI1.4 ME1.1		6.1.4						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MON:SG1.SP3 Establish Monitoring Requirements Subpractices 1. Establish monitoring requirements for the operational resilience management process. 2. Identify the level and type of monitoring activities required to meet monitoring requirements. 3. Establish parameters for requirements refresh and review.				CAM:SP2.1 CAM:SP2.2 PMC:SP1	ME1.2 ME1.3 PO3.3	BCP Pro-cess	4.3 6.2.1 6.2.2	6.4.4 6.4.5.2 6.4.5.3 6.4.5.4	10.10.1 10.10.2 10.10.4 10.10.5 13.2.1			5.4.2 5.6.2 5.7.2	
MON:SG1.SP4 Analyze and Prioritize Monitoring Requirements Subpractices 1. Analyze monitoring requirements. 2. Assign priority to monitoring requirements. 3. Identify monitoring requirements that may not be able to be satisfied. 4. Identify risks that result from unsatisfied requirements.				PMC:SP1	ME1.3		4.3 6.2.2						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MON:SG2 Perform Monitoring													
MON:SG2.SP1 Establish and Maintain Monitoring Infrastructure Subpractices 1. Identify and inventory existing monitoring infrastructure and capabilities that may address the program objectives and monitoring requirements. 2. Identify infrastructure needs to support accepted requirements. 3. Implement and manage monitoring infrastructure.				CAM:SP2.1 CAM:SP2.2 PMC:SP1	ME1.4 ME2.1 DS13.3 PO10.9	BCP Pro-cess	6.3.2	6.4.4 6.4.5.2 6.4.5.3 6.4.5.4 6.14.10 7.5.6 7.5.8	10.10.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MON:SG2.SP2 Establish Collection Standards and Guidelines Subpractices 1. Develop and maintain standards and parameters for collection of monitoring data. 2. Develop and maintain standards and parameters for the handling and storage of monitoring data collected. 3. Review, refine, and develop monitoring operating procedures.				PMC:SP1	AI3.2 AI2.3 ME1.3 DS13.3		6.3.2	6.4.4 6.4.5.2 6.4.5.3 7.5.6	10.6.1 10.10.1 10.10.2 10.10.4 10.10.5 13.2.1 15.3.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MON:SG2.SP3 Collect and Record Information Subpractices 1. Develop collection methods and procedures. 2. Assign resources to monitoring processes. 3. Monitor, collect, and record data. 4. Establish and maintain policies for proper handling, labeling, and information classification of data collected during monitoring activities.				CAM:SP2.1 CAM:SP2.2 PMC:SP1	DS3.5 DS5.5 DS13.3 ME1.2 ME2.1 ME2.2 PO3.3		6.2.3 6.3.2 6.6.7	6.4.4 6.14.10 7.5.6 9.1	10.6.1 10.10 12.2.1 12.2.2 12.2.4 12.5.4 13.2.1 15.3.1			5.4.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
MON:SG2.SP4 Distribute Information Subpractices 1. Identify media and methods of distribution based on requirements. 2. Develop and document plans, processes, and procedures for distribution of information to internal and external stakeholders. 3. Develop infrastructure to meet distribution requirements. 4. Distribute monitoring information according to requirements.				CAM:SP2.3 PMC:SP1	ME1.5		6.2.3 6.6.7						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD – Organizational Process Definition													
OPD:SG1 Establish Organizational Process Assets													
OPD:SG1.SP1 Establish Standard Processes Subpractices 1. Decompose each standard process into constituent process elements to the detail needed to understand and describe the process. 2. Specify the critical attributes of each process element. 3. Specify the relationships of the process elements. 4. Ensure that the organization's set of standard processes adheres to applicable process policies, standards, and models. 5. Ensure that the organization's set of standard processes satisfies the process needs and objectives of the organization.			OPD:SP1.1	OPD:SP1.1	AI3.1 AI4.1 AI5.1 DS1.1 DS13.1 PO3.1 PO3.2 PO4.1 PO6.3 PO10.2	Risk Monitoring and Testing						5.1.1 5.3 5.5.5 6.4.1 6.4.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP1 Establish Standard Processes Subpractices (continued) 6. Ensure that there is appropriate integration among the processes that are included in the organization's set of standard processes. 7. Document the organization's set of standard processes. 8. Conduct peer reviews on the organization's set of standard processes. 9. Revise the organization's set of standard processes as necessary.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP2 Establish Tailoring Criteria and Guidelines Subpractices 1. Specify the selection criteria and procedures for tailoring the organization's set of standard processes. 2. Specify the standards for documenting the defined processes. 3. Specify the procedures for submitting and obtaining approval of waivers from the requirements of the organization's set of standard processes. 4. Document the tailoring guidelines for the organization's set of standard processes. 5. Conduct peer reviews on the tailoring guidelines. 6. Revise the tailoring guidelines as necessary.			OPD:SP1.2	OPD:SP1.2									

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP3 Establish the Organization's Measure-ment Repository			OPD:SP1.3	OPD:SP1.3									
Subpractices 1. Determine the organization's needs for storing, retrieving, and analyzing measurements. 2. Define a common set of process and product measures for the organization's set of standard processes. 3. Design and implement the measurement repository. 4. Specify procedures for storing, updating, and retrieving measures. 5. Conduct peer reviews on the definitions of the common set of measures and procedures for storing and retrieving measures. 6. Enter the specified measures into the repository.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP3 Establish the Organization's Measure-ment Repository Subpractices (continued) 7. Make the contents of the measurement repository available for use by the organization and operating units as appropriate. 8. Revise the measurement repository, common set of measures, and procedures as the organization's needs change.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP4 Establish the Organization's Process Asset Library Subpractices 1. Design and implement the organization's process asset library, including the library structure and support environment. 2. Specify the criteria for including items in the library. 3. Specify the procedures for storing and retrieving items. 4. Enter the selected items into the library and catalog them for easy reference and removal. 5. Make the items available for use by operating units. 6. Periodically review the use of each item and use the results to maintain the library contents. 7. Revise the organization's process asset library as necessary			OPD:SP1.4	OPD:SP1.4	DS1.1 DS1.2								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP5 Establish Work Environment Standards			OPD:SP1.5	OPD:SP1.5	PO6.4								
Subpractices 1. Evaluate the commercially available environment standards appropriate for the organization. 2. Adopt existing work environment standards and develop new ones to fill gaps based on the organization's process needs and objectives.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPD:SG1.SP6 Establish Rules and Guidelines for Integrated Teams Subpractices 1. Establish and maintain empowerment mechanisms to enable timely decision making. 2. Establish rules and guidelines for structuring and forming integrated teams. 3. Define the expectation, rules, and guidelines that guide how integrated teams work collectively. 4. Maintain the rules and guidelines to help team members balance their team and home organizational responsibilities.			IPM+IPPD: SP3.3 IPM+IPPD: SP3.4 OPD+IPPD: SP2.2 OPD+IPPD: SP2.3		AI1.4 PO10.3								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF – Organizational Process Focus													
OPF:SG1 Determine Process Improvement Opportunities													
OPF:SG1.SP1 Establish Organizational Process Needs Subpractices 1. Identify policies, standards, and business objectives that are applicable to the organization's processes. 2. Examine relevant process standards and models for best practices. 3. Determine the organization's process performance objectives. 4. Define the essential characteristics of the organization's processes. 5. Document the organization's process needs and objectives. 6. Revise the organization's process needs and objectives as needed.			OPF:SP1.1	OPF:SP1.1	AI1.1 ME2.2 ME4.3 ME4.4 PO10.1 PO10.2 PO10.5			9.1 9.4.1				4.6 5.5.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG1.SP2 Appraise the Organization's Processes Subpractices 1. Obtain sponsorship of the process appraisal from higher-level managers. 2. Define the scope of the process appraisal. 3. Determine the method and criteria to be used for the process appraisal. 4. Plan, schedule, and prepare for the appraisal process. 5. Conduct the process appraisal. 6. Document the appraisal's activities and deliver the findings.			OPF:SP1.2	OPF:SP1.2	DS13.2 ME2.1 ME2.2 ME4.3 ME4.4 PO10.2 PO10.13	Business Impact Analysis		9.1					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG1.SP3 Identify the Organization's Process Improvements Subpractices 1. Determine candidate process improvements. 2. Prioritize candidate process improvements. 3. Identify and document the process improvements to be implemented. 4. Revise the list of planned process improvements and keep it current.			OPF:SP1.3	OID:SP1.1 OPF:SP1.3	AI1.3 DS8.5 DS13.2 ME2.7 ME4.3 ME4.4 PO10.13			9.1					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG2 Plan and Implement Process Actions													
OPF:SG2.SP1 Establish Process Action Plans Subpractices 1. Identify strategies, approaches, and actions to address identified process improvements. 2. Establish process action teams to implement actions. 3. Document process action plans.			OPF:SP2.1	OPF:SP2.1	DS8.5 DS13.2 PO10.6			9.4.2	10.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG2.SP2 Implement Process Action Plans Subpractices 1. Make process action plans readily available to relevant stakeholders. 2. Negotiate and document commitments among process action teams and revise their progress action plans as necessary. 3. Track progress and commitments against process action plans. 4. Conduct joint reviews with process action teams and relevant stakeholders to monitor the progress and results of process actions. 5. Plan pilots needed to test selected process improvements. 6. Review the activities and work products of process action teams. 7. Identify, document, and track to closure issues encountered when implementing process action plans.			OPF:SP2.2	OID:SP1.3 OPF:SP2.2	DS8.5 PO10.6								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG2.SP2 Implement Process Action Plans Subpractices (continued) 8. Ensure that results of implementing process action plans satisfy the organization's process improvement objectives.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG3 Deploy Organizational Process Assets and Incorporate Experiences													
OPF:SG3.SP1 Deploy Organizational Process Assets Subpractices 1. Deploy organizational process assets across the organization. 2. Document changes to organizational process assets. 3. Deploy changes that were made to organizational process assets across the organization. 4. Provide guidance and consultation on the use of organizational process assets.			OPF:SP3.1	OPF:SP3.1		Risk Monitoring and Testing							

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG3.SP2 Deploy Standard Processes Subpractices 1. Identify organizational units in the organization that are starting up or recently acquired. 2. Identify existing organizational units that would benefit from implementing the organization's current set of standard processes. 3. Establish plans to implement the organization's current set of standard processes in the identified organizational units. 4. Assist organizational units in tailoring the organization's set of standard processes to meet their needs. 5. Maintain records of tailoring and implementing processes for the identified organizational units.			OPF:SP3.2	OID:SP2.1 OPF:SP3.2									

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG3.SP2 Deploy Standard Processes Subpractices (continued) 6. Ensure the defined processes resulting from process tailoring are incorporated into plans for process-compliance audits. 7. As the organization's set of standard processes is updated, identify which organizational units should implement the changes.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG3.SP3 Monitor the Implementation Subpractices 1. Monitor use of the organization's process assets (including standard processes) and changes to them. 2. Review selected process assets. 3. Review results of process compliance audits to determine how well the organization's set of standard processes has been deployed. 4. Identify, document, and track to closure issues related to implementing the organization's set of standard processes.			OPF:SP3.3	OID:SP2.2 OPF:SP3.3	DS8.5 PO4.3 PO10.13	Risk Monitoring and Testing						8.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets			OPF:SP3.4	OPF:SP3.4	DS8.5	Risk Monitoring and Testing						8.2	
Subpractices 1. Conduct periodic reviews of effectiveness and suitability of the organization's set of standard processes and related organizational process assets relative to the organization's strategic objectives. 2. Obtain feedback about the use of organizational process assets. 3. Derive lessons learned from defining, piloting, implementing, and deploying organizational process assets. 4. Make lessons learned available to staff as appropriate. 5. Analyze measurement data obtained from the use of the organization's common set of measures.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OPF:SG3.SP4 Incorporate Experiences into Organizational Process Assets Subpractices (continued) 6. Appraise processes, methods, and tools in use in the organization and develop recommendations for improving organizational process assets. 7. Make the best of the organization's processes, methods, and tools available to staff as appropriate. 8. Manage process improvement proposals. 9. Establish and maintain records of the organization's process improvement activities.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA – Organizational Training and Awareness													
OTA:SG1 Establish Awareness Program													
OTA:SG1.SP1 Establish Awareness Needs Subpractices 1. Analyze the organization's resilience program to identify the types and extent of awareness training that are necessary to satisfy resilience program objectives. 2. Document the awareness training needs of the organization by staff group. 3. Determine the resources necessary to meet the awareness needs. 4. Revise the awareness needs of the organization as changes to the resilience program and strategy are made.		10.2			PO6.5		3.3.1 3.3.2 3.3.3	9.2					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG1.SP2 Establish Awareness Plan Subpractices 1. Establish awareness training plan content. 2. Establish commitments to plan. 3. Determine resources necessary to carry out the plan. 4. Revise plan and commitments as necessary.		5.5 10.2			PO3.3		3.3.1 3.3.2	9.2	5.1.1 6.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG1.SP3 Establish Awareness Delivery Capability Subpractices 1. Select the appropriate approaches to satisfy specific organizational awareness needs based on staff group. 2. Determine whether to develop the awareness materials internally, acquire them externally, or some combination. 3. Develop or obtain awareness materials. 4. Develop or obtain qualified instructors or facilitators as needed. 5. Deliver internal communications about planned awareness activities. 6. Revise the awareness materials and supporting artifacts as necessary.		10.2			PO3.3		3.3.1 3.3.2 3.3.3	5.9.4 9.2.3	6.1.7				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG2 Conduct Awareness Activities													
OTA:SG2.SP1 Perform Awareness Activities Subpractices 1. Determine the mix of awareness activities. 2. Plan and schedule awareness activities, including regular awareness presentations. 3. Perform logistics planning for each scheduled awareness activity. 4. Assign resources to each scheduled awareness activity. 5. Perform awareness activities according to the schedule and the plan. 6. Track the delivery of awareness activities against the plan and schedule.		10.2					6.6.6	5.6.2 5.9.4 5.9.5 9.2	6.1.7 8.2.1 8.2.2 10.8.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG2.SP2 Establish Awareness Records Subpractices 1. Keep records of all awareness activities conducted throughout the organization. 2. Make awareness activity records available to appropriate people or processes.								5.6.2 5.9.5 9.2.3					
OTA:SG2.SP3 Assess Awareness Program Effectiveness Subpractices 1. Assess staff awareness level based on the staff member's respective job responsibilities and roles. 2. Provide a mechanism for evaluating the effectiveness of each awareness activity with respect to the objectives for that activity. 3. Document suggested improvements to the awareness plan and program based on the evaluation of the effectiveness of the awareness activities.								5.9.6				7.1 7.2 7.5	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG3 Establish Training Capability													
OTA:SG3.SP1 Establish Training Needs Subpractices 1. Collect information about skills gap, cross-training, and succession planning by reviewing the job responsibilities of personnel involved in resilience processes as well as current performance levels. 2. Analyze the organization's resilience requirements, goals, and objectives to determine future training needs. 3. Determine the roles and skills necessary to perform the standard processes that constitute the resilience management system. 4. Document the resilience training needs of the organization. 5. Document the training necessary to perform the roles in the organization's set of standard operational resilience management processes.		7.3 10.3	OT:SP1.1 OT:SP1.2	OT:SP1.1 OT:SP1.2	AI4.2 AI4.3 AI4.4 AI7.1 DS7.1 DS13.1 PO7.4	Board and Senior Manage-ment Re-sponsibility Other Policies, Standards, and Pro-cesses		5.9 6.4.6 6.10.6 7.5.8				6.11	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG3.SP1 Establish Training Needs Subpractices (continued) 6. Revise the resilience training needs of the organization as necessary.													
OTA:SG3.SP2 Establish Training Plan Subpractices 1. Establish resilience training plan content. 2. Establish commitments to the resilience training plan. 3. Revise plan and commitments as necessary.		5.5 7.3 10.3	OT:SP1.3	OT:SP1.3	DS7.1 PO7.4	Other Policies, Standards, and Pro-cesses		5.9.2 5.9.3 5.9.4 5.9.5	6.1.2			6.11.1 6.11.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG3.SP3 Establish Training Capability Subpractices 1. Select the appropriate approaches to satisfy specific organizational training need and competencies. 2. Determine whether to develop training materials internally or acquire them externally. 3. Develop or obtain training materials. 4. Develop or obtain qualified instructors. 5. Describe the training in the organization's training curriculum. 6. Revise the training materials and supporting work products as necessary.		10.3	OT:SP1.4	OT:SP1.4	DS7.2 PO7.4			5.9.1 5.9.2 5.9.3					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG4 Conduct Training													
OTA:SG4.SP1 Deliver Training Subpractices 1. Select the staff who will receive the training necessary to perform their roles effectively. 2. Schedule the training, including any resources, as necessary (e.g., facilities and instructors). 3. Conduct the training. 4. Track the delivery of training against the plan.		7.3 10.3	OT:SP2.1	OT:SP2.1	AI4.2 AI4.3 AI4.4 AI7.1 DS7.2 DS13.1			5.9.1 5.9.2 5.9.3 5.9.5 6.3.9 6.4.6 6.10.6 7.5.8	8.2.2 10.8.1 11.7.1 11.7.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG4.SP2 Establish Training Records Subpractices 1. Keep records of all staff (including external entities), indicating whether or not they successfully completed each training course or other approved training activity. 2. Keep records of all staff who have been waived from specific training. 3. Keep records of all staff who successfully complete their designated required training. 4. Make training records available to the appropriate people or processes.			OT:SP2.2	OT:SP2.2	DS7.3			5.9.5					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
OTA:SG4.SP3 Assess Training Effectiveness Subpractices 1. Provide a mechanism for assessing the effectiveness of each training course with respect to established organizational, project, or individual learning (or performance) objectives. 2. Collect other data that can be used to evaluate training effectiveness. 3. Document suggested improvements to the training plan based on the evaluation of the effectiveness of training activities.			OT:SP2.3	OT:SP2.3	DS7.3			5.9.6 6.4.6				7.1 7.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM – People Management													
PM:SG1 Establish Vital Staff													
PM:SG1.SP1 Identify Vital Staff Subpractices 1. Identify vital service-support staff. 2. Identify vital resilience-focused staff 3. Identify vital managers. 4. Identify staff who have access to, control of, or protection responsibility for highly valuable or highly sensitive organizational assets. 5. Identify other vital staff. 6. Reconcile the lists of vital staff periodically to service continuity plans and other resilience-focused strategies. 7. Periodically validate and update the lists of vital staff based on changes in the operational and organizational environment.		6.4 8.7.3			PO4.13 PO7.5	Appendix G: BCP Compo-nents							

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG2 Manage Risks Associated with Staff Availability													
PM:SG2.SP1 Identify and Assess Staff Risk Subpractices 1. Determine the scope of risk assessment for staff. 2. Identify risks to the availability of staff. 3. Analyze risks to the availability of staff. 4. Categorize and prioritize staff risks. 5. Assign a risk disposition to each staff risk. 6. Monitor the risk and the risk strategy on a regular basis to ensure that it does not pose additional threat to the organization. 7. Develop a strategy for those risks that the organization decides to mitigate.		7.3			PO7.5	Risk Man-agement		6.4.16 6.6.2 6.10.7 6.12.5.2 6.13.5				5.2.7 5.4.3 5.6.1 5.6.2 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG2.SP2 Mitigate Staff Risk Subpractices 1. Develop and implement risk mitigation strategies for all risks that have a "mitigation" or "control" disposition. 2. Validate the risk mitigation plans by comparing them to existing strategies. 3. Identify the person or group responsible for each risk mitigation plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan. 4. Address residual risk. 5. Implement the risk mitigation plans and provide a method to monitor the effectiveness of these plans. 6. Monitor risk status. 7. Collect performance measures on the risk management process.		7.3			PO7.5	Risk Man-agement		6.4.16 6.10.7 6.12.5.2 6.13.5				5.6.1 5.6.2 5.6.3 5.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG3 Manage the Availability of Staff													
PM:SG3.SP1 Establish Redundancy for Vital Staff Subpractices 1. Determine which vital staff positions must have redundancy. 2. Identify backup staff for vital staff positions. 3. Develop strategic plan for providing staff redundancy. 4. Provide training to redundant staff to perform necessary roles and responsibilities.		7.3			PO4.12 PO4.13 PO7.5		6.3.1	6.3.9					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG3.SP2 Perform Succession Planning Subpractices 1. Identify key positions that need to be included in succession planning. 2. Develop strategies for creating a succession chain. 3. Establish detailed succession plans for key personnel positions. 4. Mentor and train successor personnel to perform necessary functions.		7.3			PO4.13 PO7.4 PO7.5		6.3.1	6.3.9					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG3.SP3 Prepare for Redeployment Subpractices 1. Establish plans for staff redeployment during disruptive events. 2. Notify staff of the plans for their redeployment during disruptive events. 3. Provide appropriate training for staff in advance of redeployment. 4. Obtain and provide credentials for first responders. 5. Review and update plans for staff redeployment during disruptive events as needed.		7.3			DS4.8								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG3.SP4 Plan to Support Staff During Disruptive Events Subpractices 1. Establish a strategy for support considerations during disruptive events. 2. Identify areas of support that the organization must provide. 3. Develop plans to support staff during disruptive events. 4. Assign resources to the plans to support staff during disruptive events. 5. Review and update the plans to support staff during disruptive events as needed.		6.2.3			DS4.8			5.2 5.5.5 6.10.7 6.13 9.4.3					

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
PM:SG3.SP5 Plan for Return-to-Work Considerations								5.2 9.4.3					
Subpractices 1. Establish a strategy for transitioning staff back to the workplace. 2. Identify and procure resources that will be needed to ensure effective transition. 3. Review and revise the plans to address return-to-work considerations after a disruptive event as appropriate.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK – RISK Management													
RISK:SG1 Prepare for Risk Management													
RISK:SG1.SP1 Determine Risk Sources and Categories Subpractices 1. Determine operational risk sources. 2. Determine operational risk categories. 3. Create an operational risk taxonomy.		6.5	RSKM:SP1.1	RSKM:SP1.1	ME4.5	Risk Assessment Risk Management Appendix F: Business impact analysis process	6.6.5 6.6.7	9.5.1	4.1	8.2.1.3		5.3 5.4.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG1.SP2 Establish an Operational Risk Management Strategy Subpractices 1. Develop and document an operational risk management strategy that aligns with the organization's overall enterprise risk management strategy. 2. Communicate the operational risk management strategy to relevant stakeholders and obtain their commitment to the activities.	4.3.1	6.5	RSKM:SP1.3	RSKM:SP1.3	ME4.5 PO9.1	BCP Process Risk Management Appendix F: Business impact analysis process t	4.1.4 6.6.3 6.6.4 6.6.5	5.11 9.5.1	4.1 14.1.1	7.1 9.4 9.5 10	5.1 5.2 5.3.1 5.3.2 5.3.3 5.3.4	5.4	
RISK:SG2 Establish Risk Parameters and Focus													
RISK:SG2.SP1 Define Risk Parameters Subpractices 1. Define risk thresholds for each risk category. 2. Establish risk management parameters.		6.2.3 6.5	RSKM:SP1.2	RSKM:SP1.2	ME4.5 PO9.2	Risk Assessment Risk Management Appendix F: Business impact analysis process		6.2.7	4.1	7.2	5.3.5		

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG2.SP2 Establish Risk Measurement Criteria Subpractices 1. Define organizational impact areas. 2. Prioritize impact areas for the organization. 3. Define and document risk measurement and evaluation criteria. 4. Define and document risk likelihood.		6.2.3 6.5			ME4.5 PO9.2 PO9.5	Risk As-sessment Risk Man-agement Appendix F: Business impact analysis process	6.6.4	6.2.7	4.2	7.2 7.3 7.4 8.2.2.1	5.3.5	5.3.2 5.4.2 5.4.3 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG3 Identify Risk													
RISK:SG3.SP1 Identify Asset-Level Risks Subpractices 1. Identify the tools, techniques, and methods that the organization can use to identify operational risks to organizational assets. 2. Identify the operational risks (at the asset level) that can negatively impact high-value organizational services. 3. Develop risk statements. 4. Identify the relevant stakeholders associated with each documented risk.	4.2.1	6.5	RSKM:SP2.1	RSKM:SP2.1	AI1.2 PO9.3 PO9.4 PO10.9	Risk Assessment Risk Management Appendix F: Business impact analysis process	6.6.4	5.4 5.5.1 6.2.7	4.1 12.1.1 14.1.1 14.1.2	8.1 8.2.1.6	5.4.2	5.3.1 5.3.2 5.4.3 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG3.SP2 Identify Service-Level Risks Subpractices 1. Identify the services that are associated with each asset-specific risk statement. Update the risk statement to reflect associated services. 2. Determine the effect on the service that could result from the realization of risk at the asset level. 3. Update risk statement information to reflect service-specific consequences and the severity of the consequences due to realized risk.	4.2.1	6.5	RSKM:SP2.1	RSKM:SP2.1	AI1.2 PO9.3 PO9.4 PO10.9	Risk Assessment Risk Management Appendix F: Business impact analysis process		5.4 5.5.1 6.2.7	4.1 12.1.1 14.1.1 14.1.2	8.1 8.2.1.6	5.4.2	5.4.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG4 Analyze Risk													
RISK:SG4.SP1 Evaluate Risk Subpractices 1. Evaluate the identified risks using the defined risk parameters and risk measurement criteria. 2. Assign a valuation to each risk statement.	4.2.1 4.3.1	5.5 6.6	RSKM:SP2.2	RSKM:SP2.2	AI1.2 PO9.4 PO10.9	Risk Assessment Risk Management Appendix F: Business impact analysis process		5.4 5.5.1 6.2.7	4.1	8.2.2.2 8.2.2.3 8.2.2.4	5.4.3	5.3.1 5.4.3 5.4.4 5.6.3	
RISK:SG4.SP2 Categorize and Prioritize Risk Subpractices 1. Categorize and group risks according to the defined risk categories or other classification. 2. Prioritize risks for disposition and mitigation.	4.3.1	6.6	RSKM:SP2.2	RSKM:SP2.2	AI1.2 PO9.4	Risk Assessment Appendix F: Business impact analysis process			4.2	8.1 8.2.2.5	5.4.4 5.4.4		

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG4.SP3 Assign Risk Disposition Subpractices 1. Assign a risk disposition to each risk statement based on risk valuation and prioritization. 2. Obtain approval for the proposed disposition of each risk, particularly those that are not going to be mitigated. 3. Develop a strategy to carry out the proposed risk disposition. 4. Monitor the risk and the risk strategy on a regular basis to ensure that it does not pose additional threat to the organization. 5. Develop a strategy for those risks that the organization decides to mitigate.		6.6 6.7	RSKM:SP2.2	RSKM:SP2.2	PO9.4 PO9.5	Appendix F: Business impact analysis process	8.3.3 8.3.4			8.1 9.3 10	5.4.4		

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG5 Mitigate and Control Risk													
RISK:SG5.SP1 Develop Risk Mitigation Plans Subpractices 1. Develop risk mitigation plans for all risks that have a mitigation or control disposition. 2. Validate the risk mitigation plans by comparing them to existing protection and sustainability strategies. 3. Identify the person or group responsible for each risk mitigation plan and ensure they have the authority to act and the proper level of skills and training to implement and monitor the plan. 4. Address residual risk.		6.6.4 7.1 7.2	RSKM:SP3.1	RSKM:SP3.1	PO9.6	Risk Man-agement		5.11 6.2.10 9.5.1	4.2	9.1	5.5.1 5.5.2	5.6.1 5.6.2 5.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG5.SP2 Implement Risk Strategies Subpractices 1. Monitor risk status. 2. Provide a method for tracking open risks to closure. 3. Implement the risk mitigation plans and provide a method to monitor the effectiveness of these plans. 4. Provide continued commitment of resources for each plan to allow successful execution of the risk management activities. 5. Collect performance measures on the risk management process.		6.6.4 6.6.5 7.1 7.2	RSKM:SP3.2	RSKM:SP3.2	PO9.6 PO10.9	Risk Management		5.11	4.2	9.1	5.5.3		

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG6 Use Risk Information to Manage Resilience													
RISK:SG6.SP1 Review and Adjust Strategies to Protect Assets and Services Subpractices 1. Compare risk mitigation plans to existing control structures for affected assets and services. 2. Revise existing controls or develop and implement additional controls that are necessary to mitigate risks.		6.6			PO9.6	BCP Process Risk Assessment Risk Management Risk Monitoring and Testing	8.3.8 8.3.9			9.2 10 12	5.6 5.7	5.6.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RISK:SG6.SP2 Review and Adjust Strategies to Sustain Services Subpractices 1. Compare risk mitigation plans to existing continuity of operations plans for affected assets and services. 2. Revise existing continuity of operations plans or develop and implement additional plans that are necessary to mitigate risks.		6.6			PO9.6	BCP Process Risk Assessment Risk Management Risk Monitoring and Testing	8.3.8 8.3.9			9.2 10 12	5.6 5.7		

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRD – Resilience Requirements Development													
RRD:SG1 Identify Enterprise Requirements													
RRD:SG1.SP1 Establish Enterprise Resilience Requirements Subpractices 1. Consult legal, statutory, regulatory, and contractual requirements that an organization and all of its external entities are required to satisfy. 2. Identify business-specific constraints. 3. Identify the principles, objectives, and business requirements for processing, storing, and transmitting information that an organization has developed to support its operations. 4. Identify organizational strategic objectives, critical success factors, policies or other indicators of importance that could result in enterprise requirements.			RD:SP1.1 RD:SP1.2 RD:SP2.3		AI1.1 PO10.12	Other Policies, Standards, and Pro-cesses	4.1.2 4.1.4		5.1.1 6.1.1 12.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRD:SG1.SP1 Establish Enterprise Resilience Requirements													
Subpractices (continued) 5. Develop and communicate a list of enterprise requirements that affect all organizational units and lines of business.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRD:SG2 Develop Service Requirements													
RRD:SG2.SP1 Establish Asset Resilience Requirements Subpractices 1. Interview asset owners to determine specific asset-level requirements. 2. Perform information security risk assessment and/or business impact analysis to identify risks that must be reflected in asset requirement. 3. Document confidentiality, integrity, and availability requirements for each service-related asset.			RD:SP2.1		DS4.8	Other Policies, Standards, and Pro-cesses	4.1.1 4.1.2 4.1.4	5.3.3 6.3.3	6.1.1 7.1.3 12.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRD:SG2.SP2 Assign Enterprise Resilience Requirements to Services Subpractices 1. Identify enterprise-level requirements that are applicable to each service and associated asset. 2. Assign enterprise-level requirements to services and associated assets.			RD:SP2.2		DS4.8	Other Policies, Standards, and Processes	4.1.1 4.1.2 4.1.4		6.1.1 7.1.3 12.1.1				
RRD:SG3 Analyze and Validate Requirements													
RRD:SG3.SP1 Establish a Definition of Required Functionality Subpractices 1. Document the asset functionality description for each asset that is associated with one or more services.			RD:SP3.1 RD:SP3.2			BCP Process	4.1.1 4.1.2 4.1.4						

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRD:SG3.SP2 Analyze Resilience Requirements Subpractices 1. Analyze asset requirements against baseline asset functionality and identify conflicts. Make adjustments to requirements as necessary. 2. Develop conflict mitigation action plans to resolve requirements deficiencies and conflicts that result from analysis and validation activities. 3. Analyze asset requirement against enterprise requirements that have been assigned to services. Revise asset requirements to reflect enterprise requirements to reflect enterprise requirements where necessary.			RD:SP3.3 RD:SP3.4				4.1.4		6.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRD:SG3.SP3 Validate Resilience Requirements			RD:SP3.5				4.1.4		6.1.1				
Subpractices 1. Perform affinity analysis between strategic drivers (such as critical success factors) and asset requirements. 2. Critically analyze requirements to ensure that they adequately specify what is needed to protect and sustain an asset relative to its association with a service. 3. Identify requirement gaps. 4. Revise requirements as necessary.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRM – Resilience Requirements Management													
RRM:SG1 Manage Requirements													
RRM:SG1.SP1 Obtain an Understanding of Resilience Requirements Subpractices 1. Establish objective criteria for the evaluation and acceptance of requirements. 2. Analyze requirements to ensure that the established evaluation and acceptance criteria are met. 3. Reach an understanding (between owners and custodians) on the requirements so that custodians can commit to them.		7.1	REQM:SP1.1	REQM:SP1.1	PO10.12		4.1.1 4.1.2 4.1.4		6.1.1 7.1.3 12.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRM:SG1.SP2 Obtain Commitment to Resilience Requirements Subpractices 1. Document and communicate requirements through service-level agreements between asset owners and custodians. 2. Document the custodian's understanding of requirements and obtain sign-off.			REQM:SP1.2	REQM:SP1.2			4.1.1 4.1.2 4.1.4		7.1.3 12.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRM:SG1.SP3 Manage Resilience Requirements Changes			REQM:SP1.3	REQM:SP1.3			4.1.2						
Subpractices							4.1.3						
1. Establish a requirements baseline from which changes will be managed.							4.1.4						
2. Develop and document criteria for establishing when a change in requirements must be considered.							9.1.1						
3. Analyze results of information security risk assessment and/or business impact analysis to identify changes to requirements that are related to risk mitigation.													
4. Document the requirements changes.													
5. Maintain a requirement change history with rationale for performing the changes.													
6. Evaluate the impact of requirement changes on existing protection and sustainability activities and commitments.													
7. Establish communications channels to ensure custodians are aware of changes in requirements.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRM:SG1.SP4 Maintain Traceability of Resilience Requirements			REQM:SP1.4	REQM:SP1.4			9.1.1						
Subpractices 1. Document requirements and their source or origin as part of asset profile or documentation. 2. Maintain requirements traceability. 3. Generate a requirements traceability matrix.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RRM:SG1.SP5 Identify Inconsistencies Between Resilience Requirements and Activities Performed to Meet the Requirements			REQM:SP1.5	REQM:SP1.5			4.1.2 4.1.4						
Subpractices 1. Review the planned or implemented activities for consistency with requirements. 2. Document custodial constraints that may impede satisfaction of requirements and update requirements as necessary. 3. Identify changes that have to be made in activities (or planned activities) to ensure satisfaction of requirements as specified. 4. Initiate corrective actions to enforce alignment between requirements and activities.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RTSE – Resilient Technical Solution Management													
RTSE:SG1 Establish Guidelines for Resilient Technical Solution Development													
RTSE:SG1.SP1 Identify General Guidelines Subpractices 1. Identify general guidelines for the development of resilient software and systems.			TS:SP1.1		AI2.1 PO8.1				10.3.1 12.2 12.3				
RTSE:SG1.SP2 Identify Requirements Guidelines Subpractices 1. Identify requirements guidelines for the development of resilient software and systems.			TS:SP1.2		AI1.1 PO8.1								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RTSE:SG1.SP3 Identify Architecture and Design Guidelines Subpractices 1. Identify requirements guidelines for the development of resilient software and systems.			TS:SP2.1 TS:SP2.2		AI2.1 AI2.2 PO8.3				10.3.1 12.2 12.3				
RTSE:SG1.SP4 Identify Implementation Guidelines Subpractices 1. Identify coding guidelines for the development of resilient software. 2. Identify testing guidelines for the development of resilient software. 3. Identify testing guidelines for the development of resilient systems.			TS:SP2.3		AI1.1 AI2.2 PO8.3				12.2 12.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RTSE:SG1.SP5 Identify Assembly and Integration Guidelines					AI2.2 PO8.3				10.3.2 12.4.1				
Subpractices 1. Identify coding guidelines for the development of resilient software.													
RTSE:SG2 Develop Resilient Technical Solution Development Plans													
RTSE:SG2.SP1 Select and Tailor Guidelines			TS:SP2.4										
Subpractices 1. Identify selection criteria for resilience guidelines. 2. Select and tailor guidelines for specific software or system asset.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RTSE:SG2.SP2 Integrate Selected Guidelines with a Defined Software and System Development Process Subpractices 1. Update process definitions. 2. Update development plan.			TS:SP2.4		AI2.7								
RTSE:SG3 Execute the Plan													
RTSE:SG3.SP1 Monitor Execution of the Development Plan Subpractices 1. Monitor project performance against the development plan to ensure that resilience requirements are satisfied. 2. Update development project plans, resilience guidelines, and process definitions as appropriate.			TS:SP3.1		AI2.8 PO8.5								

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
RTSE:SG3.SP2 Release Resilient Technical Solutions into Production			TS:SP3.1 TS:SP3.2		AI7.8								
Subpractices 1. Establish inspection criteria. 2. Inspect software and systems to ensure they have satisfied inspection criteria. 3. Approve assets for release.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC – Service Continuity													
SC:SG1 Prepare for Service Continuity													
SC:SG1.SP1 Plan for Service Continuity Subpractices 1. Establish the plan for managing service continuity. 2. Establish commitments to the plan. 3. Revise the plan and commitments as necessary.	4.3.3 4.4.7	4.1,2,3,4 5.1,2,3 7.1-7.10 8.6 8.7 9.5.3			DS4.1	BCP Process Board and Senior Management Responsibility Other Policies, Standards, and Processes Appendix D: Pandemic Planning Appendix G: BCP Components	6.3.1 6.3.3	5.1 5.3.3,4 5.4 5.5.2 5.8.1 5.11 6.1 6.4.15 9.4.1,2 9.5.2	14.1.1 14.1.4			4.1 4.2 4.3 4.4 5.1.1 5.2 6.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG1.SP2 Establish Standards and Guidelines for Service Continuity Subpractices 1. Develop and communicate service continuity management guidelines and standards.	4.4.3 4.5.4	4.1 4.2, 4.3 4.4 5.1 5.2 5.3 5.5			DS4.1	BCP Process Board and Senior Management Responsibility Business Impact Analysis Risk Management Other Policies, Standards, and Processes Appendix G: BCP Components	6.3.3	5.5.2 5.8.1 5.8.4 5.8.5 5.11 6.1 6.3.14 6.4.15 9.4.2 9.5.2	14.1.4 5.1.1			4.4 5.2 6.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG2 Identify and Prioritize High-Value Services													
SC:SG2.SP1 Identify the Organization's High-Value Services Subpractices 1. Identify the organization's high-value services, associated assets, and activities. 2. Analyze and document the relative value of providing these services and the resulting impact on the organization if these services are interrupted. 3. Prioritize and document the list of high-value services that must be provided if a disruption occurs.		4.4 6.2.1 6.3		SCON:SP1.1	DS4.2 DS4.3	BCP Process Business Impact Analysis Appendix E: Interdependencies Appendix G: BCP Components	6.3.4	5.3.1 9.5.1	14.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG2.SP2 Identify Internal and External Dependencies and Interdependencies Subpractices 1. Identify and document internal infrastructure dependencies that the organization relies upon to provide services. 2. Identify and document external entities that the organization relies upon to provide services. 3. Develop a key contact list for organizational services that can be included as part of the service continuity plans.		4.5 6.1.2 6.2.2		SCON:SP1.2		BCP Process Business Impact Analysis Risk Management Appendix G: BCP Components	6.3.4	5.5.1 5.5.2				5.2.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG2.SP3 Identify Vital Organizational Records and Databases Subpractices 1. Identify and document vital records and databases. 2. Identify and document vital staff and their specific roles in relation to the services being provided. 3. Ensure that vital records and databases are protected, accessible, and usable in the event of a disruption or interruption.		6.2 6.3 6.4 6.5 6.6 7.6 8.7.5		SCON:SP1.1		BCP Pro-cess	6.3.4	5.3.1 5.8.4	10.5.1 10.8.5 15.1.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG3 Develop Service Continuity Plans													
SC:SG3.SP1 Identify Plans to Be Developed Subpractices 1. Identify service continuity plans to be developed.		4.3 5.4.2 5.5 7.2 8.7.2		SCON:SP2.1	DS4.2 DS4.3	Board and Senior Management Responsibility Appendix D: Pandemic Planning Appendix G: BCP Components	6.3.3	9.4.2 9.5.2	14.1.3 14.1.4			5.2 6.4.2 6.7.2 6.9.3 6.9.5	
SC:SG3.SP2 Develop and Document Service Continuity Plans Subpractices 1. Document the service continuity plans using available templates as appropriate. 2. Document the key elements of the specific plan. 3. Identify the stakeholders of specific service continuity plans.	4.4.4 4.4.6	4.2 5.5 7.2		SCON:SP2.1	DS4.2 DS4.3	Board and Senior Management Responsibility Risk Management Appendix G: BCP Components	6.3.3 6.3.4	5.3.4 5.8.4 5.8.5 5.12 9.4.2 9.5.2	14.1.3 14.1.4			5.2 6.7.2 6.9.3 6.9.5	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG3.SP3 Assign Staff to Service Continuity Plans Subpractices 1. Identify staff requirements to satisfy the objectives of the service continuity plans. 2. Identify staff, both internal and external, to satisfy the resource requirements. 3. Assign staff to the service continuity plans.		5.2 6.4 8.3.3 8.7.3 8.7.4			DS4.3	Board and Senior Management Responsibility Other Policies, Standards, and Processes Appendix G: BCP Components	6.3.4	5.8.4				5.2.2 5.2.3 5.2.4 5.2.5	
SC:SG3.SP4 Store and Secure Service Continuity Plans Subpractices 1. Establish a service continuity plan inventory or database. 2. Store and protect the service continuity plans in the plan inventory or database. 3. Establish access controls to ensure that service continuity plans can only be accessible to authorized individuals.	4.4.5 4.5.4	8.3.1			DS4.7	Risk Management	6.3.4	5.12	14.1.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG3.SP5 Develop Service Continuity Plan Training Subpractices 1. Identify any specialized training needs based on skill gaps for the activities as described in the plan. 2. Develop a strategy for conducting service continuity plan training. 3. Develop training materials and resources to conduct plan training on a regular and ongoing basis. 4. Train resources as necessary to fulfill their responsibilities in the plan. 5. Update service continuity plans, if necessary, as a result of feedback from training.		5.3.1 10.2 10.3		SCON:SP2.2 SCON:SP2.3	DS4.6 DS4.7	Board and Senior Manage-ment Re-sponsibility	6.3.4	5.9.2		14.1.5		6.11.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG4 Validate Service Continuity Plans													
SC:SG4.SP1 Validate Plans to Requirements and Standards Subpractices 1. Review plans for consistency in achieving stated resilience requirements for associated services and assets. 2. Review plans for adherence to service continuity plan development standards and guidelines. 3. Identify plan omissions, gaps, and issues and develop appropriate plan updates and remediation actions.		4.3 5.4.1		SCON:SP3.1 SCON:SP3.2 SCON:SP3.3	DS3.4 DS4.4	Board and Senior Management Responsibility Risk Management						7.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG4.SP2 Identify and Resolve Plan Conflicts Subpractices 1. Review plans to determine plan conflicts. 2. Determine the severity of plan conflicts and develop appropriate mitigation actions to reduce or eliminate the conflict. 3. Rewrite or revise plans as necessary.		5.4.1			DS4.5	Board and Senior Management Responsibility Risk Management							
SC:SG5 Exercise Service Continuity Plans													
SC:SG5.SP1 Develop Testing Program and Standards Subpractices 1. Develop testing program and test standards to apply universally across all testing of service continuity plans. 2. Establish schedules for ongoing testing and review of plans.	4.5.2.2	9.1 9.2 9.3			DS4.5	Board and Senior Management Responsibility Risk Management Risk Monitoring and Testing Appendix H: Testing Program - Governance and Attributes	6.3.4	5.9.3 5.10	4.6 14.1.5			7.1	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG5.SP2 Develop and Document Test Plans Subpractices 1. Develop and document service continuity plan tests. 2. Review service continuity test plans with stakeholders.		5.4.1 5.5 9.2		SCON:SP2.1	AI7.2 DS4.5	Board and Senior Management Responsibility Risk Management Risk Monitoring and Testing Appendix H: Testing Program - Governance and Attributes	6.3.4	5.9.3 5.10 6.15.4	10.5.1 14.1.5			7.2 7.3 7.4 7.5	
SC:SG5.SP3 Exercise Plans Subpractices 1. Prepare to conduct service continuity plan tests. 2. Execute the service continuity plan test. 3. Document and record the results in accordance with the organization's testing standards.		5.4.1		SCON:SP2.1	DS4.5	Board and Senior Management Responsibility Risk Monitoring and Testing Appendix H: Testing Program - Governance and Attributes	6.3.4	5.9.3 5.10 6.15.4	14.1.5			7.4	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG5.SP4 Evaluate Plan Test Results Subpractices 1. Compare actual test results with expected test results and test objectives. 2. Document areas of improvement for service continuity plans. 3. Document areas of improvement for testing service continuity plans	4.5.3	5.4.1 9.3.2		SCON:SP3.3	DS4.5	Board and Senior Management Responsibility Risk Assessment Risk Management Risk Monitoring and Testing Appendix H: Testing Program - Governance and Attributes	6.3.4	5.10 6.15.4	14.1.5			7.5	
SC:SG6 Execute Service Continuity Plans													
SC:SG6.SP1 Execute Plans Subpractices 1. Determine the conditions under which a service continuity plan must be executed. 2. Execute plans as required.		8.3.4				Risk Assessment Risk Management Risk Monitoring and Testing Appendix A: Examination Procedures							

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG6.SP2 Measure the Effectiveness of the Plans in Operation Subpractices 1. Compare documented plan results with plan objectives and expectations. 2. Document areas of improvement for service continuity plans. 3. Document areas of improvement for testing service continuity plans.	4.5.3	9.4 9.5		SCON:SP3.3	DS4.10	Risk Assessment Risk Management Risk Monitoring and Testing Appendix A: Examination Procedures		9.1				8.1	
SC:SG7 Maintain Service Continuity Plans													
SC:SG7.SP1 Establish Change Criteria Subpractices 1. Develop and document criteria for establishing when changes to a service continuity plan should be considered.		9.5			DS4.4	Board and Senior Management Responsibility BCP Process Risk Management	6.3.4	5.10 9.1	14.1.5			8.1.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
SC:SG7.SP2 Maintain Changes to Plans Subpractices 1. Identify and document changes to the service continuity plans based on defined criteria and conditions. 2. Increment versions of the service continuity plan in the plan inventory/database. 3. Communicate the updated plan to appropriate stakeholders as required.		5.4.1 5.4.2 8.3.5 9.4 9.5			DS4.4	Board and Senior Management Responsibility BCP Process Risk Management			14.1.5			8.2	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM – Technology Management													
TM:SG1 Establish and Prioritize Technology Assets													
TM:SG1.SP1 Prioritize Technology Assets Subpractices 1. Compile a list of high-value technology assets from the organization's technology asset inventory. 2. Prioritize technology assets. 3. Periodically validate and update the list of high-value technology assets based on operational and organizational environment changes.		6.4											

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG1.SP2 Establish Resilience-Focused Technology Assets Subpractices 1. Compile a list of resilience-focused technology assets from the organization's asset inventory. 2. Periodically reconcile the list of resilience-focused technology assts to the organization's service continuity plans and resilience strategies.		6.4 8.7.3			DS4.8 PO3.4		9.1.2	5.3.1,2 6.6.4 6.7.1,6 6.8.1 6.11.2 6.12.2.4 6.12.2.5 6.12.3,4 6.12.5.3,4 6.12.5.5,6 6.12.6	12.1.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG2 Protect Technology Assets													
TM:SG2.SP1 Assign Resilience Requirements to Technology Assets Subpractices 1. Assign resilience requirements to technology assets. 2. Document the requirements (if they are currently not documented) and include in the asset definition.					AI2.4 AI7.3 AI7.4 DS4.8 DS5.7 PO3.4		6.1.2	5.3.3 6.6.1,4 6.7.1 6.8.4 6.8.5.4,5 6.8.6 6.9.1,2 6.10.6 6.12.2.4,5 6.12.3,4 6.12.5.3,4 6.12.5.5,6 6.12.6 7.6.6,8	10.8.5 12.4.2 12.4.3 12.5.1 12.5.2 12.5.4				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG2.SP2 Establish and Implement Controls Subpractices 1. Establish and implement administrative controls for technology assets. 2. Establish and implement technical controls for technology assets. 3. Establish and implement physical controls for technology assets. 4. Establish and specify controls over the design, construction, or acquisition of technology assets. 5. Monitor the effectiveness of administrative, technical, and physical controls, and identify deficiencies that must be resolved.					AI2.3 AI2.4 AI2.5 AI3.2 AI7.3 AI7.4 DS5.7			6.3.3 6.3.5,6,7 6.6.2,4 6.7.1 6.8.4 6.8.5.4 6.8.5.5 6.8.6 6.9.1,2 6.10.6 6.12.2.4,5 6.12.3,4 6.12.5.3 6.12.5.4 6.12.5.5 6.12.5.6 6.12.6 7.6.8	9.2 10.1.2 10.6.1,2 10.7.2 10.8 10.9.1,3 10.10.2,3 10.10.6 11.3.2,3 11.4 11.5.1,3,4 11.5.5,6 11.6.2 11.7.1,2 12.2.2,3,4 12.4.1,2,3 12.5.1,2,4 15.1.3,4,5 15.3.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG3 Manage Technology Asset Risk													
TM:SG3.SP1 Identify and Assess Technology Asset Risk Subpractices 1. Determine the scope of risk assessment for technology assets. 2. Identify risks to technology assets. 3. Analyze risks to technology assets. 4. Categorize and prioritize risks to technology assets. 5. Assign a risk disposition to each technology asset risk. 6. Monitor the risk and the risk strategy on a regular basis to ensure that it does not pose additional threat to the organization. 7. Develop a strategy for those risks that the organization decides to mitigate.					PO9.1 PO9.4	Risk Man-agement		6.7.4 6.9.3	10.10.2 11.7.1 11.7.2 15.1.3			5.4.3 5.6.1 5.6.2 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG3.SP2 Mitigate Technology Risk Subpractices 1. Develop and implement risk mitigation strategies for all risks that have a "mitigation" or "control" disposition. 2. Validate the risk mitigation plans by comparing them to existing protection and sustainability strategies. 3. Identify the person or group responsible for each risk mitigation plan and ensure that they have the authority to act and the proper level of skills and training to implement and monitor the plan. 4. Address residual risk. 5. Implement the risk mitigation plans and provide a method to monitor the effectiveness of these plans. 6. Monitor risk status. 7. Collect performance measures on the risk management process.					PO9.4 PO9.5	Risk Management		6.7.4	11.7.1 11.7.2 15.1.3			5.6.1 5.6.2 5.6.3 5.7	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG4 Manage Technology Asset Integrity													
TM:SG4.SP1 Control Access to Technology Assets Subpractices 1. Establish access management policies and procedures for requesting and approving access privileges to technology assets. 2. Establish organizationally acceptable tools, techniques, and methods for controlling access to technology assets. 3. Identify and document staff who are authorized to modify technology assets relative to the asset's resilience requirements. 4. Implement tools, techniques, and methods to monitor and log modification activity on high-value technology assets. 5. Perform periodic audits of technology asset modification logs, and identify and address anomalies.				CM:SP1.2			6.1.2	6.12.2.2	10.1.2 10.1.4 10.9.3 10.10.3 11.5.4 12.4.1 12.4.2 12.4.3 12.5 15.1.3 15.3.1 15.3.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG4.SP2 Perform Configuration Management Subpractices 1. Establish requirements for technology standards, guidelines, and policies for configuration management. 2. Establish a configuration management database or system. 3. Identify the technology assets (configuration items) in detail that will be placed under configuration management. 4. Create baseline configuration items. 5. Track and control changes to configuration items. 6. Review configuration control logs and identify anomalies. 7. Perform configuration audits.			CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1 CM:SP3.2	CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1 CM:SP3.2	AI2.6 DS9.1 DS9.2 DS9.3		6.1.2 9.1.1 9.1.3 9.1.4 9.1.5 10.1.7		10.1.2 10.9.3 11.5.4 12.4.1 12.5.1 15.1.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG4.SP3 Perform Change Control and Management Subpractices 1. Develop and implement change control policies, procedures, and techniques. 2. Initiate and record change requests in the change control database or system. 3. Analyze the impact of changes proposed in the change requests. 4. Obtain agreement and approval for changes to baselines from relevant stakeholders. 5. Track the status of change requests to closure. 6. Control configuration items.			CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1 CM:SP3.2	CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1 CM:SP3.2	AI6.1 AI6.2 AI6.3 AI6.4 AI6.5 AI7.6 AI7.9		6.1.2 9.1.1 9.1.3 9.1.4 9.2.1 9.2.2 9.2.3 9.2.4 10.1.4 10.1.5 10.1.6 10.1.7 10.1.8 10.1.9		10.1.2 10.9.1 10.9.3 12.4.1 12.5.1 12.5.2 15.1.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG4.SP4 Perform Release Management Subpractices 1. Develop and implement guidelines for the appropriate planning and release of technology assets. 2. Plan technology asset releases. 3. Develop release "builds." 4. Test release "builds." 5. Move release "builds" into the organization's production environment.			CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1 CM:SP3.2 SAM:SP2.5	CM:SP1.2 CM:SP1.3 CM:SP2.1 CM:SP2.2 CM:SP3.1 CM:SP3.2 SAM:SP2.5	AI7.7 AI7.8		6.1.2 9.1.1 9.1.4 10.1.1 10.1.2 10.1.3 10.1.4 10.1.5 10.1.6 10.1.7 10.1.8 10.1.9		10.1.2 10.3.2 10.9.3 12.4.1 12.5				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG5 Manage Technology Asset Availability													
TM:SG5.SP1 Perform Planning to Sustain Technology Assets Subpractices 1. Develop an approach for sustaining technology assets. 2. Establish availability metrics for key technology assets. 3. Establish recovery time objectives for high-value technology assets. 4. Establish recovery point objectives for high-value technology assets. 5. Develop service continuity plans that address technology availability.		7.5		CAM:SP1.1			6.1.2 6.3.1	5.5.3 5.5.4 6.7.3 6.7.4 6.8.3 6.8.5.1 6.8.5.2 6.8.5.3	15.1.3				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG5.SP2 Manage Technology Asset Maintenance Subpractices 1. Identify technology systems that require regular maintenance activities. 2. Document equipment supplier's recommended service intervals and specifications. 3. Document a list of maintenance personnel authorized to carry out repairs and service. 4. Document all suspected or actual faults and all preventative, corrective, or other types of maintenance. 5. Implement maintenance and test maintenance changes in a non-operational environment when appropriate. 6. Establish appropriate controls over sensitive or confidential information when maintenance is performed.				CAM:SP1.1	AI3.3 AI2.10 DS13.5		6.1.2	7.6.4	9.2.4 10.8.1 10.8.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG5.SP2 Manage Technology Asset Maintenance Subpractices (continued) 7. Communicate maintenance change notification to appropriate parties. [CMMI-SVC] 8. Implement maintenance according to change request procedures. 9. Document and communicate results of maintenance.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG5.SP3 Manage Technology Capacity Subpractices 1. Identify technology assets that require capacity management and planning. 2. Document technology asset use, performance, capacity, and availability needs. 3. Forecast technology asset use, performance, capacity, and availability needs. 4. Develop a strategy to meet the demand for capacity based on the resilience requirements for the technology asset and the services it supports. 5. Periodically validate and update the capacity management strategy for technology assets based on operational and organizational environment changes.				CAM:SP1.1 CAM:SP2.3	DS3.1 DS3.2 DS3.3 DS3.4 DS3.5		6.1.2 6.5	6.7.5 6.8.1 6.8.3 6.8.5.1 6.8.5.2 6.8.5.3 6.10.1 6.14.8	10.3.1				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
TM:SG5.SP4 Manage Technology Interoperability					AI3.4				10.3.2				
Subpractices 1. Establish interoperability standards. 2. Develop interoperability management strategy. 3. Identify and analyze risks related to interoperability of technology assets. 4. Monitor the interoperability strategy on a regular basis to ensure that it does not pose additional risks to the organization.													

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
VAR – Vulnerability Analysis and Resolution													
VAR:SG1 Prepare for Vulnerability Analysis and Resolution													
VAR:SG1.SP1 Establish Scope Subpractices 1. Identify the assets that are the focus of vulnerability analysis and resolution activities. 2. Identify the operational environments where vulnerabilities may exist for each asset. 3. Define the scope of vulnerability analysis and resolution activities.						Appendix C: Internal and external threats Appendix F: Business impact analysis process		5.2	12.6.1			5.4.2.2 5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy Subpractices 1. Develop and document an operational vulnerability analysis and resolution strategy. 2. Communicate the operational vulnerability analysis to relevant stakeholders and obtain their commitment to the activities described in the strategy. 3. Assign resources to specific vulnerability analysis and resolution roles and responsibilities. 4. Identify the tools, techniques, and methods that the organization will use to identify vulnerabilities to assets.						Appendix C: Internal and external threats Appendix F: Business impact analysis process			10.4.1 10.4.2 12.6.1			5.6.3	

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
VAR:SG2 Identify and Analyze Vulnerabilities													
VAR:SG2.SP1 Identify Sources of Vulnerability Information Subpractices 1. Identify sources of relevant vulnerability information. 2. Review sources on a regular basis and update as necessary.						Appendix F: Business impact analysis process			10.8.5 12.5.2				5.6.3
VAR:SG2.SP2 Discover Vulnerabilities Subpractices 1. Discover vulnerabilities. 2. Provide training to staff to perform data collection and discover vulnerabilities. 3. Populate the vulnerability repository. 4. Provide access to the vulnerability repository to appropriate process stakeholders.					DS5.5 DS5.9 PO9.1		8.3.1		6.1.2 12.5.2 12.6.1 15.2.2	8.2.1.5			

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
VAR:SG2.SP3 Analyze Vulnerabilities Subpractices 1. Develop prioritization guidelines for vulnerabilities. 2. Analyze the structure and action of the vulnerability. 3. Prioritize and categorize vulnerabilities for disposition. 4. Update the vulnerability repository with analysis and prioritization/ categorization information.						Appendix F: Business impact analysis process	8.3.1 8.3.10		10.8.5 12.6.1 13.1.2				

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
VAR:SG3 Manage Exposure to Vulnerabilities													
VAR:SG3.SP1 Manage Exposure to Vulnerabilities Subpractices 1. Develop a vulnerability management strategy for all vulnerabilities that require resolution. 2. Ensure that relevant stakeholders are informed of resolution activities. 3. Update the vulnerability repository with information on the vulnerability management strategy. 4. Monitor the status of open vulnerabilities. 5. Analyze the effectiveness of vulnerability management strategies to ensure that objectives are achieved.					DS5.9		8.3.3 8.3.8 8.3.9 8.3.10			9.1.6			

CERT® Resilience Management Model v1.1	Commercial Standards and Practices												
Process Area Specific Goals and Specific Practices	ANSI/ASIS SPC.1-2009	BS25999-1: 2006	CMMI-Dev	CMMI-Svc	COBIT 4.1	FFIEC BCP Handbook	ISO/IEC 20000-2: 2005 (E)	ISO/IEC 24762: 2008 (E)	ISO/IEC 27002: 2005 (E)	ISO/IEC 27005: 2008 (E)	ISO/IEC 31000: 2009 (E)	NFPA 1600	PCI: 2009
VAR:SG4 Identify Root Causes													
VAR:SG4.SP1 Perform Root-Cause Analysis Subpractices 1. Identify and select root cause tools, techniques, and methods appropriate for use in analyzing the underlying causes of vulnerabilities. 2. Identify and analyze the root causes of vulnerabilities. 3. Develop and implement strategies to address root causes. 4. Monitor the effects of implementing strategies to address root causes.							8.3.1						

References/Bibliography

URLs are valid as of the publication date of this document.

[ANSI 2009]
American National Standards Institute, Inc. / ASIS International. *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*. ASIS International, 2009 (ISBN 978-1-887056-92-2).

[BSI 2006]
The British Standards Institution. *Business Continuity Management, Part 1: Code of Practice*. BSI, 2006 (ISBN 0 580 49601 5).

[BSI 2007]
The British Standards Institution. *Business Continuity Management, Part 2:Specification*. BSI, 2007 (ISBN 978 0 580 59913 2).

[CMMI 2006]
CMMI Product Team. *CMMI for Development, Version 1.2* (CMU/SEI-2006-TR-008). Software Engineering Institute, Carnegie Mellon University, 2006.

[CMMI 2009]
CMMI Product Team. *CMMI for Services, Version 1.2* (CMU/SEI-2009-TR-001). Software Engineering Institute, Carnegie Mellon University, 2009.

[FFIEC 2008]
Federal Financial Institutions Examination Council. "Business Continuity Planning." *IT Examination Handbook*. FFIEC, 2008.

[ISO/IEC 2005a]
ISO/IEC. *Information Technology—Service Management—Part 2: Code of Practice* (ISO/IEC 20000-2:2005). International Organization for Standardization, 2005.

[ISO/IEC 2005b]
ISO/IEC. *Information Technology—Security Techniques—Code of Practice for Information Security Management* (ISO/IEC 27002:2005). International Organization for Standardization, 2005.

[ISO/IEC 2008a]
ISO/IEC. *Information technology—Security techniques—Guidelines for Information and Communications Technology Disaster Recovery Services* (ISO/IEC 24762:2008). International Organization for Standardization, 2008.

[ISO/IEC 2008b]
ISO/IEC. *Information technology—Security techniques—Information Security Risk Management* (ISO/IEC 27005:2008). International Organization for Standardization, 2009.

[ISO/IEC 2009]
ISO/IEC. *Risk management – Principles and Guidelines* (ISO/IEC 31000:2009). International Organization for Standardization, 2009.

[ITGI 2007]
IT Governance Institute. *COBIT 4.1*. ITGI, 2007.

[NFPA 2007]
National Fire Protection Association. *NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs*. NFPA, 2007.

[PCI 2007]
Payment Card Industry (PCI) Data Security Standard, Version 1.1 (Release: September 2006). Provided courtesy of PCI Security Standards Council, LLC and/or its licensors. ©2007 PCI Security Standards Council, LLC. All Rights Reserved.

[PCI 2009]
PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard (PCI DSS)*, Version 1.2.1 (Release: July 2009). PCISSC, 2009.
Provided courtesy of PCI Security Standards Council, LLC and/or its licensors. ©2009 PCI Security Standards Council, LLC. All Rights Reserved. The current version of the PCI DSS is available at http://www.pcisecuritystandards.org.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	October 2011	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1	FA8721-05-C-0003

6. AUTHOR(S)

Kevin G. Partridge
Lisa R. Young

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2011-TN-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

CERT® Resilience Management Model (CERT-RMM) provides a reference model that allows organizations to make sense of their practice deployment in a process context. In this context, the primary goal of this document is to help model users and adopters to understand how CERT-RMM process areas, industry standards, and codes of practices that are used by organizations in an operational setting are connected. Additionally, this document helps to achieve a primary goal of CERT-RMM, which is to allow adopters to continue to use their preferred standards and codes of practice at a tactical level while maturing management and improvement of operational resilience at a process level. This document was also created with the objective to permit organizations to use CERT-RMM as a means for managing the complexities of deploying more than one standard or code of practice.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CERT-RMM crosswalk of practices, practice bodies, ANSI/ASIS SPC.1-2009, BS 25999, COBIT 4.1, CMMI-SVC, CMMI-DEV, FFIEC Business Continuity Planning Handbook, ISO/IEC 20000-2:2005 (E), ISO/IEC 24762:2008 (E), ISO/IEC 27002:2005 (E), ISO/IEC 27005:2008 (E), ISO/IEC 31000:2009 (E), NFPA 1600, PCI-DSS	254

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL